1/2020

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

43. Jahrgang
ISSN 0137-7767
14,00 Euro



■ Der Betriebsarzt und der Datenschutz ■ Verarbeitung von Gesundheits- und Sozialdaten ■ „Digitale-Versorgung-Gesetz" und Datentransparenz ■ Datenschutz in der Klinik ■ 1000 Schritte zur alltäglichen Überwachung ■ Implantateregister-Errichtungsgesetz ■ Pressemitteilungen ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



~~Donnerstag, 30. April 2020~~ [verschoben auf Herbst 2020]
Big Brother Awards
Stadttheater Bielefeld

Freitag, 01. Mai 2020
Redaktionsschluss DANA 2/2020
„e-Payment“

Mittwoch/Donnerstag 06./07. Mai 2020
BvD-Verbandstage 2020 „Datenschutz: Made in Europe – ein globaler Standard“

Samstag, 01. August 2020:
Redaktionsschluss DANA 3/2020
„eGovernment – Datenschutz in öffentlichen Stellen“

Sonntag, 01. November 2020
Redaktionsschluss DANA 4/2020
„Mobilität“

Foto: Pixabay..com

DANA
Datenschutz Nachrichten
ISSN 0137-7767
43. Jahrgang, Heft 1

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftsstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Heinz Alenfelder
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autorinnen und Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0) 91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 14 Euro. Jahresabonnement 48 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta,
Pixabay, iStock

Editorial


Bild: iStock

Aktuell ist die Gesundheit allerorten dank der Corona-Pandemie ein Gesprächsthema. In Zeiten nicht nur virtueller globaler Vernetzung können aus lokal auftretenden Krankheiten schnell Epidemien werden, wie uns COVID-19 gerade deutlich zeigt. Die Pläne für diese Schwerpunktausgabe wurden allerdings recht früh im letzten Jahr gemacht und dieses Heft kann und will vor allem eines nicht leisten: die Lieferung tagesaktueller Information zu Gesetzen und immer neuen Gesetzesvorhaben der Berliner Regierungskoalition.

Vielmehr werden Hintergründe beleuchtet sowie Fakten und Auslegungen geliefert, indem das „Digitale-Versorgung-Gesetz" detailliert betrachtet wird, die Datenschutzaspekte bei Auftragsverarbeitung von Gesundheits- und Sozialdaten herausgearbeitet werden und schließlich die Datenverarbeitung durch die Dienstleistungsfirma ACTINEO kritisch analysiert wird. Die umfassende rechtliche Beleuchtung der Position eines Betriebsarztes rundet das Schwerpunktthema ab. Außerdem versuchen wir in diesem Heft ein für die DANA neues Format, das Interview, und hinterfragen die alltägliche Datenschutzsituation eines Arztes im Krankenhaus.

Zum Weiterlesen können sowohl die Meldungen als auch die Buchbesprechungen anregen, die den Schluss dieser Ausgabe bilden. Datenschutz-Themen, die Sie hier nicht finden, sind vielleicht im letzten Jahr schon in der DANA behandelt worden. Deshalb empfehlen wir einen Blick ins beigeheftete Jahresregister 2019 und verabschieden uns mit dem Wunsch, dass Sie alle gesund bleiben mögen!

Die DANA-Redaktion

Autorinnen und Autoren dieser Ausgabe:

Heinz Alenfelder
Vorstandsmitglied in der DVD,
alenfelder@datenschutzverein.de, Köln

Werner Hülsmann
Vorstandsmitglied in der DVD, huelsmann@datenschutzverein.de, Ismaning

Mike Kuketz
Pentester und Lehrbeauftragter für IT-Sicherheit, www.kuketz-blog.de

Dr. Thilo Weichert
Vorstandsmitglied in der DVD, Netzwerk Datenschutzexpertise,
weichert@datenschutzverein.de, Kiel

Thilo Weichert

Der Betriebsarzt und der Datenschutz



Bild: iStock

Die Datenverarbeitung durch Betriebsärzte weist gegenüber anderer medizinischer Datenverarbeitung die Besonderheit auf, dass nicht nur das Medizinrecht und das Datenschutzrecht zur Anwendung kommen, sondern zudem das Arbeitsrecht mit seinen spezifischen Regelungen. Mit der europäischen Datenschutz-Grundverordnung (DSGVO) kam zusätzlich zur nationalen eine europäische Regelungsebene hinzu, was die Anwendung der Normen nicht einfacher macht. Im Folgenden sollen die wesentlichen Regeln in ihrer praktischen Umsetzung dargestellt werden.

1. Datenschutz-Grundverordnung

Die europäische Datenschutz-Grundverordnung (DSGVO) ist auf betriebsärztliche Datenverarbeitung umfassend anzuwenden, da hierbei personenbezogene Daten verarbeitet werden (Art. 2 DSGVO).

Die Verarbeitung personenbezogener Gesundheitsdaten ist in Art. 9 DSGVO geregelt unter dem zusammenfassenden Begriff der „besonderen Kategorien personenbezogener Daten". Hierzu gehören u. a. auch genetische Daten, biometrische Daten zur eindeutigen Personenidentifizierung sowie Daten zum Sexualleben.

Als Erlaubnistatbestände für die Verarbeitung dieser besonderen Datenkategorien werden in Art. 9 Abs. 2 DSGVO u. a. genannt: die ausdrückliche Einwilligung (lit. a), die Erforderlichkeit, damit „aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des sozialen Rechtsschutzes erwachsende Rechte" ausgeübt werden können (lit. b), der Schutz „lebenswichtiger Interessen" der Betroffenen (lit. c), die Erforderlichkeit „zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen" (lit. f), „für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich" (lit. h), „aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit" (lit. i) oder für „Forschungszwecke" (lit. j).

Art. 9 Abs. 3 DSGVO enthält zudem eine Regelung zur Verarbeitung von Daten, die einem Berufsgeheimnis unterliegen, so wie dies im deutschen Recht für die Verarbeitung durch Betriebsärzte zutrifft. Danach ist es den nationalen Gesetzgebern erlaubt, verstärkte Geheimhaltungspflichten festzulegen.[1]

Sowohl Art. 9 Abs. 2 lit. b, h, i und j als auch Art. 9 Abs. 3 DSGVO enthalten Öffnungsklauseln, wonach eine präzisierende nationale Rechtsgrundlage möglich, ja evtl. sogar nötig ist. Dies bedeutet, dass die vor dem Wirksamwerden der DSGVO geltenden spezifischen Regelungen in Deutschland zu sensitiven Daten weitgehend weitergelten konnten.[2] Tatsächlich wurden von den deutschen Gesetzgebern auf Bundes- und auf Landesebene die insofern relevanten Regelungen inhaltlich nicht geändert.

Zur Umsetzung der Öffnungsklauseln der DSGVO und Anpassung des nationalen Rechts an die DSGVO mussten aber die allgemeinen Datenschutzgesetze, also auf Bundesebene das Bundesdatenschutzgesetz (BDSG), geändert werden.[3] In § 22 BDSG ist die „Verarbeitung besonderer Kategorien personenbezogener Daten" geregelt. Die Norm paraphrasiert in Abs. 1 weitgehend Art. 9 Abs. 2 DSGVO sowie in Abs. 2 die Anforderungen an „angemessene und spezifische Maßnahmen" der Technik und der Organisation, wie sie insbesondere in den Art. 25, 32 DSGVO geregelt sind.[4] Eine für die ärztliche Datenverarbeitung bedeutsame Regelung ist zudem die Einschränkung der Kontrollbefugnisse der Datenschutzaufsichtsbehörden bei Berufsgeheimnisträgern (§ 29 Abs. 3 BDSG).

Art. 88 DSGVO, der die „Datenverarbeitung im Beschäftigtenkontext" regelt, enthält eine weitere Öffnungsklausel. Deren Umsetzung erfolgte in § 26 BDSG, der in den Absätzen 1 und 3 eine weitgehende Paraphrasierungen des Art. 88 Abs. 1 DSGVO bzgl. der Verarbeitungszwecke vornimmt und in Abs. 2 die Voraussetzungen für wirksame Einwilligungen im Beschäftigtenkontext präzisiert. § 26 Abs. 7 BDSG stellt klar, dass die datenschutzrechtlichen Regeln unabhängig davon gelten, ob die Beschäftigtendaten in einem (digitalen) Dateisystem oder in (Papier-) Akten gespeichert sind und verarbeitet werden. Als Rechtsgrundlage für die Verarbeitung kommen auch Kollektivvereinbarungen (Dienst- bzw. Betriebsvereinbarungen, Tarifverträge) in Betracht (Art. 88 Abs. 1 DSGVO, § 26 Abs. 4 BDSG), wobei diese die allgemeinen Abwägungsregeln zwischen den Arbeitgeberinteressen und den Grundrechten der betroffenen Beschäftigten beachten

müssen.[5] Für die betriebsärztliche Datenverarbeitung gibt es also zwei Öffnungsklauseln (Art. 9 u. 88 DSGVO).[6]

Mit der DSGVO sind nunmehr viele allgemeine Fragen zur Datenverarbeitung durch den Betriebsarzt abgedeckt, so zur Verantwortlichkeit, zur Begründung der Betroffenenrechte oder zur Datenschutzkontrolle generell. Das neue BDSG ist relevant als Auffangregelung, soweit nicht spezifische Gesetze präzisere Regelungen enthalten, sowie für Beschränkungen der Betroffenen- und der Kontrollrechte (§§ 29, 32-37 BDSG).

2. Verantwortlichkeit

Gemäß Art. 4 Nr. 4 DSGVO ist „'Verantwortlicher' die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". Es kommt auf die juristische Sichtweise an: Die natürliche oder juristische Person, die über Zweck und Mittel der Verarbeitung bestimmt, ist verantwortlich.[7] Dabei ist es nicht nötig, dass die Stelle objektiv und umfassend über die Daten bestimmen kann, nicht einmal, dass sie direkt darauf Zugriff hat.[8] Voraussetzung für die Verantwortlichkeit ist, dass die Stelle willentlich, evtl. in Kooperation mit anderen gemeinsam Verantwortlichen, einen kausalen Beitrag für die Datenverarbeitung leistet.

Der Betriebsarzt wird gemäß § 2 Abs. 1 Arbeitssicherheitsgesetz (ASiG) vom Arbeitgeber bestimmt. Der Arbeitgeber sorgt dafür, dass die von ihm bestellten Betriebsärzte ihre Aufgaben erfüllen und stellt die hierfür nötigen „Räume, Einrichtungen, Geräte und Mittel zur Verfügung" (§ 2 Abs. 2 ASiG). Zu den Aufgaben des Betriebsarztes gehört es, „die Arbeitnehmer zu untersuchen, arbeitsmedizinisch zu beurteilen und zu beraten sowie die Untersuchungsergebnisse zu erfassen und auszuwerten" (§ 3 Abs. 1 Nr. 2 ASiG).

Arbeitsmedizin ist geprägt von einem Dreiecksverhältnis zwischen Arbeitgeber, Beschäftigten und Betriebsarzt. Dabei geht es in Bezug auf die Verarbeitung von Daten darum, dass dem Arbeitgeber die für die Erbringung der Arbeitsleistung und die Bereitstellung des Arbeitsplatzes erforderlichen Informationen zur Verfügung gestellt werden und zugleich der Persönlichkeitsschutz der Beschäftigten und deren Vertrauensverhältnis zum medizinischen Personal gewahrt werden.[9] Zur datenschutzrechtlichen Verantwortlichkeit enthält das Arbeitssicherheitsgesetz (ASiG) keine Aussage, weshalb insofern auf die allgemeinen Normen der DSGVO zurückzugreifen ist. Danach ist zu unterscheiden, ob der Betriebsarzt Mitarbeiter des Arbeitgebers ist (interner Betriebsarzt) oder seine Dienste als unabhängiger Dienstleister zur Verfügung stellt (externer Betriebsarzt).[10]

Ist der Betriebsarzt Mitarbeiter des Arbeitgebers (interner Betriebsarzt), so ist er Teil der vom Arbeitgeber geführten juristischen Person und somit nicht Verantwortlicher.[11] Verantwortlicher ist der Arbeitgeber. Dieser ist i. d. R. auch im sachenrechtlichen Sinn über die betriebsärztliche Dokumentation verfügungsbefugt. Dass dem Arbeitgeber wegen der ärztlichen Schweigepflicht keine Zugriffsrechte auf die Daten zustehen, spielt für die datenschutzrechtliche Einordnung keine Rolle.

Der externe Betriebsarzt, egal ob Einzelperson oder betriebsärztlicher Dienst, ist als eigenständige, vom Arbeitgeber getrennte juristische Person dagegen nicht dem Arbeitgeber zuzuordnen. Der externe Betriebsarzt bzw. betriebsärztliche Dienst ist also im Sinne des Datenschutzrechts selbst Verantwortlicher. Dies schließt nicht aus, dass er die Räumlichkeiten, Einrichtungen und Geräte des Arbeitgebers in Anspruch nimmt und der Arbeitgeber insofern deren Eigentümer ist. Es kommt darauf an, dass er als natürliche oder juristische Person vertraglich mit dem Arbeitgeber hierüber eine Vereinbarung trifft und insofern über Mittel und Zwecke der Verarbeitung (mit-)bestimmt. Möglich ist auch, dass sich die Mittel der ärztlichen Dokumentation im Eigentum des externen Betriebsarztes befinden. Der Arbeitgeber ist in Bezug auf die Verarbeitung im Rahmen der gesetzlichen Aufgabenwahrnehmung des Betriebsarztes, also nicht bei einer freiwilligen medizinischen Behandlung eines Patienten, auch (gemeinsam) Verantwortlicher, weil er gemeinsam mit dem Betriebsarzt sowohl Mittel als auch Zwecke der Verarbeitung bestimmt (Art. 26 DSGVO).

3. Arbeitsmedizin zwischen Medizin-, Arbeits- und Datenschutzrecht

Neben den datenschutzrechtlichen Anforderungen sind im Bereich der Arbeitsmedizin die des Medizinrechts zu beachten. Diese finden ihre standesrechtliche Grundlage in den Berufsordnungen der Landesärztekammern, welche sich weitgehend an der Musterordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBOÄ) orientieren.

Eine weitere Rechtsgrundlage für das Arzt-Patienten-Verhältnis ist der zivilrechtlich abgeschlossene Behandlungsvertrag, dessen Ausgestaltung mit dem Patientenrechtegesetz 2013 in den §§ 630a bis 630h Bürgerliches Gesetzbuch (BGB) ausführlich geregelt wurde. Diese Regelungen gelten für den externen Betriebsarzt, auch wenn das Vertragsverhältnis nicht zwischen Patienten und Arzt, sondern zwischen Arbeitgeber und Arzt besteht. Es handelt sich dabei in Bezug auf den beim Arbeitgeber Beschäftigten um einen unechten Vertrag zugunsten eines Dritten (vgl. § 328 BGB) bzw. um einen Vertrag mit Schutzwirkung für einen Dritten.[12] Unerheblich für die Einstufung als Behandlungsvertrag ist, dass die ärztlichen Leistungen sich vorrangig auf den Betrieb des Arbeitgebers beziehen (§ 3 Abs. 1 Nr. 1, 3, 4 ASiG) und erst in zweiter Linie, etwa bei der Untersuchung von Arbeitnehmern, auf den Probanden bzw. Patienten (§ 3 Abs. 1 Nr. 2 ASiG). Beim internen Betriebsarzt besteht zwischen diesem und dem Arbeitgeber ein Arbeitsvertrag. Auf diesen lassen sich aber die §§ 630a ff. BGB weitgehend entsprechend anwenden.

Es besteht gemäß § 11 Arbeitsschutzgesetz (ArbSchG) eine spezifische Schutzpflicht des Arbeitgebers zur „arbeitsmedizinischen Vorsorge": „Der Arbeitgeber hat den Beschäftigten auf ihren Wunsch unbeschadet der Pflichten aus anderen Rechtsvorschriften zu ermöglichen sich je nach den Gefahren für ihre Sicherheit und Gesundheit bei der Arbeit regelmäßig arbeitsmedizinisch untersuchen zu lassen, es sei denn, auf Grund der Beurteilung der Arbeitsbedingungen und der getroffenen Schutzmaßnahmen ist nicht mit einem

Gesundheitsschaden zu rechnen." Zugunsten der Beschäftigten ist zudem in § 10 ArbSchG geregelt, dass der Arbeitgeber Vorkehrungen zur ersten Hilfe und zu sonstigen Notfallmaßnahmen ergreifen muss, wozu er sich des Betriebsarztes bedienen kann.

Zu beachten ist weiterhin § 203 Strafgesetzbuch (StGB), der Verstöße gegen die berufliche Schweigepflicht mit Strafe bedroht und der für Angehörige eines Heilberufs und insbesondere für Ärzte gilt (§ 203 Abs. 1 Nr. 1 StGB). Die Verpflichtung gilt auch für Betriebsärzte (§ 8 Abs. 1 S. 3 ASiG).

Schließlich gibt es eine Vielzahl von Spezialgesetzen, die für besondere Formen der ärztlichen Behandlung wie auch der ärztlichen Dokumentation gelten. Hierzu zählen mit Bezug zum Arbeitsverhältnis die §§ 2-4 ASiG, 11 ArbSchG, 19-22 Gendiagnostikgesetz (GenDG).[13] Kommt es durch Betriebsärzte zu bestimmten Behandlungen, so gelten diese Regelungen ergänzend.

Zu den Spezialregelungen für den Bereich der arbeitsmedizinische Vorsorge gehört die Verordnung zur arbeitsmedizinischen Vorsorge (ArbMedVV).[14] Diese Verordnung verpflichtet den Arbeitgeber (§§ 3 ArbMedVV), wozu dieser sich des Betriebsarztes bedient (§ 6 ArbMedVV). In diesem Kontext werden vom Arbeitgeber Kenntnisse in Bezug auf die Arbeitsplatzverhältnisse (§ 6 ArbMedVV) sowie Vorsorgemaßnahmen in Bezug auf die Beschäftigten (§§ 4-5a ArbMedVV) eingefordert. Pflichtuntersuchungen erfolgen auch gegenüber Jugendlichen (§ 32 Abs. 1 Jugendarbeitsschutzgesetz – JArbSchG), bei Tätigkeiten im Lebensmittelbereich (§ 43 Abs. 1 Infektionsschutzgesetz), zur Ermittlung der Seediensttauglichkeit (§ 81 Seemanngesetz) sowie im Rahmen von Unfallverhütungsvorschriften der Unfallversicherungsträger (§ 15 Abs. 1 S. 1 Nr. 3 Sozialgesetzbuch – SGB – VII).[15] Wegen der Öffnungsklauseln in der DSGVO behalten sämtliche der genannten nationalen, regionalen und standesrechtlichen Regelungen ihre Wirksamkeit (s. o. 1).[16]

4. Dokumentationspflichten

Der Betriebsarzt ist nach vertraglichen, deliktischen wie berufsrechtlichen Grundlagen zur Dokumentation seiner ärztlichen Tätigkeit verpflichtet. Der Behandelnde, wozu auch der Betriebsarzt gehört, muss die Behandlung in einer „Patientenakte in Papierform oder elektronisch" dokumentieren (§ 630f Abs. 1 S. 1 BGB). „Berichtigungen und Änderungen von Eintragungen in der Patientenakte sind nur zulässig, wenn neben dem ursprünglichen Inhalt erkennbar bleibt, wann sie vorgenommen worden sind" (S. 2). Erfasst werden müssen alle „wesentlichen Maßnahmen", „insbesondere die Anamnese, Diagnosen, Untersuchungen, Untersuchungsergebnisse, Befunde, Therapien und ihre Wirkungen, Eingriffe und ihre Wirkungen, Einwilligungen und Aufklärungen. Arztbriefe sind in die Patientenakte aufzunehmen" (§ 630f Abs. 2 BGB). Diese vertraglichen Pflichten entsprechen den in § 10 Abs. 1 Musterberufsordnung für Ärzte (MBOÄ) geregelten standesrechtlichen Dokumentationspflichten „über die in Ausübung ihres Berufes gemachten Feststellungen und getroffenen Maßnahmen".

„Der Behandelnde hat die Patientenakte für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach anderen Vorschriften andere Aufbewahrungsfristen bestehen" (§ 630f Abs. 3 BGB). Diese Regelung entspricht inhaltlich vollständig § 10 Abs. 3 MBOÄ. Eine Konkretisierung bzgl. weitergehender Aufbewahrungspflichten erfolgte durch den Ausschuss für Arbeitsmedizin in der Arbeitsmedizinischen Regel (AMR) zu „Fristen für die Aufbewahrung ärztlicher Unterlagen" (AMR 6.1):[17] „Bei Tätigkeiten, bei denen nach längeren Latenzzeiten Gesundheitsstörungen auftreten können, reicht diese Aufbewahrungszeit nicht aus. Dies gilt insbesondere für ärztliche Unterlagen zu Tätigkeiten mit krebserzeugenden Gefahrstoffen (K1 und K2), für die Artikel 15 der Richtlinie 2004/37/EG des Europäischen Parlaments und des Rates vom 29. April 2004 über den Schutz der Arbeitnehmer gegen Gefährdung durch Karzinogene oder Mutagene bei der Arbeit eine Aufbewahrungsfrist von mindestens 40 Jahren vorsieht" (Nr. 1 AMR 6.1). Weitere Konkretisierungen der Aufbewahrungsfristen von mindestens 40 Jahren finden sich in Nr. 3 AMR 6.1.

Hinsichtlich der Verantwortlichkeit wird in Nr. 4. (2) AMR 6.1. klargestellt, dass es Aufgabe des Arbeitgebers ist, „dafür Sorge zu tragen, dass die Unterlagen innerhalb der Frist sicher verwahrt werden und nur für datenschutzrechtlich befugte Personen zugänglich sind". „Näheres regelt das ärztliche Berufsrecht und das Datenschutzrecht" (Nr. 4 (1) AMR 6.1.).

Bei der Dokumentation des Betriebsarztes handelt es sich materiell-rechtlich nicht um einen Teil der Personalakte, die vom Arbeitgeber zu führen ist und für die gesonderte rechtliche Regelungen gelten.[18]

In der ArbMedVV ist eine Unterscheidung zwischen der Vorsorge im Dienste der Gesundheit des Arbeitnehmers (§§ 5, 5a) und Eignungsuntersuchungen für Zwecke des Arbeitgebers (§ 4) angelegt.[19] Diese Differenzierung zwischen der Verarbeitung im vorrangigen Interesse des Arbeitnehmers und der im Interesse des Arbeitgebers sollte sich in der Struktur der Dokumentation des Betriebsarztes widerspiegeln. Angaben zu Eignungsuntersuchungen sind getrennt oder zumindest abtrennbar zu verwahren.[20]

5. Ärztliches Berufsgeheimnis

Für Betriebsärzte gilt die ärztliche Schweigepflicht des § 203 Strafgesetzbuch (StGB) bzw. § 9 MBOÄ (Patientengeheimnis). Ein Beschäftigter hat zwar – anders als beim normalen Arzt-Patienten-Verhältnis – keine freie Arztwahl. Für bestimmte Untersuchungen ist ausschließlich der Betriebsarzt zuständig. Dennoch muss die Beziehung zwischen dem Betriebsarzt und den Beschäftigten von starkem Vertrauen getragen sein, welches vom Patientengeheimnis gestützt wird.

Der Betriebsarzt hat nach § 8 Abs. 1 ArbSiG eine dem Arbeitgeber bzw. dem Dienstherrn gegenüber unabhängige Stellung und muss auch diesem gegenüber die ärztliche Schweigepflicht wahren.[21] Er darf den Arbeitgeber nur im Rahmen des für die Aufgabenwahrnehmung erforderlichen Umfangs informieren, was sich in der Regel auf die für den Arbeitgeber zu ziehenden Schlussfolgerungen beschränkt.[22] Untersuchungsergebnisse aus der allgemeinen arbeits-

medizinischen Vorsorge (§ 3 Abs. 1 Nr. 2 ASiG) bedürfen für ihre Offenbarung gegenüber dem Arbeitgeber der ausdrücklichen Einwilligung des Patienten.[23] § 26 Abs. 2 BDSG ist insofern anzuwenden. Es kommt dabei nicht darauf an, ob der Betriebsarzt intern mittels Arbeitsvertrag eingesetzt ist oder ob er allein praktizierend bzw. als Mitarbeiter eines ärztlichen Unternehmens, dessen Geschäftsfeld die Erbringung betriebsärztlicher Leistungen ist, extern tätig ist.

6. Beendigung der betriebsärztlichen Tätigkeit

§ 10 Abs. 4 MBOÄ regelt, wie mit der Dokumentation nach Beendigung der ärztlichen Tätigkeit umzugehen ist: „Nach Aufgabe der Praxis haben Ärztinnen und Ärzte ihre ärztlichen Aufzeichnungen und Untersuchungsbefunde gemäß Absatz 3 aufzubewahren oder dafür Sorge zu tragen, dass sie in gehörige Obhut gegeben werden. Ärztinnen und Ärzte, denen bei einer Praxisaufgabe oder Praxisübergabe ärztliche Aufzeichnungen über Patientinnen und Patienten in Obhut gegeben werden, müssen diese Aufzeichnungen unter Verschluss halten und dürfen sie nur mit Einwilligung der Patientin oder des Patienten einsehen oder weitergeben."

Die betriebsärztliche Dokumentation beinhaltet arbeitnehmerbezogene individuelle medizinische wie auch arbeitgeber- bzw. unternehmens- und arbeitsplatzbezogene Aspekte. Sie wird sowohl für den Patienten als auch für den Arbeitgeber geführt und kann insbesondere gegenüber den Unfallversicherungsträgern als Nachweis erfolgter Vorsorgemaßnahmen dienen. Das Patientengeheimnis steht einer Aktenübergabe an den nachfolgenden Betriebsarzt grundsätzlich nicht entgegen; datenschutzrechtlich ist die Übergabe für die weitere Aufgabenerfüllung gerechtfertigt. Bei einem Wechsel des Betriebsarztes sind die Patientenakten an den neuen Betriebsarzt zu übergeben. Dieser muss in der Lage sein, die Aufgaben seines Vorgängers für den Arbeitgeber sowie im Interesse der Beschäftigten nahtlos weiter zu erfüllen.

Eine ausdrückliche Einwilligung der Beschäftigten bzw. Patienten für den Übergang des Gewahrsams an den Akten ist nicht nötig. Allerdings ist zu beachten, dass bei einem Wechsel des Betriebsarztes den betroffenen Beschäftigten für die Teile der Akte eine Widerspruchsmöglichkeit eingeräumt wird, die der Vorgänger außerhalb einer Pflichtvorsorge angelegt hat.[24] Die medizinischen Daten, die ein Patient dem Betriebsarzt freiwillig zugänglich gemacht hat, sind für den neuen Betriebsarzt zu sperren. Dabei handelt es sich um eine medizinspezifische Form der Einschränkung der Verarbeitung (vgl. Art. 18 DSGVO). Bei einem Wechsel des Betriebsarztes darf der Nachfolger nur mit expliziter Einwilligung des Betroffenen Zugriff auf die Informationen aus Eignungsuntersuchungen nehmen (vgl. Art. 18 Abs. 2 DSGVO, § 9 Abs. 4 MBOÄ).

Der Datenbestand mit Bezug zu Vorsorgemaßnahmen geht an den neuen Betriebsarzt über. Die Zustimmung der betroffenen Beschäftigten ist nicht erforderlich. Wohl aber sind die Beschäftigten aus Transparenzgründen rechtzeitig und umfassend über den geplanten Wechsel des Betriebsarztes aufzuklären (z. B. durch Mitarbeiter-Rundschreiben).[25] Bei einem Wechsel des externen Betriebsarztes wird dies zwingend durch Art. 14 DSGVO gefordert.

Den Betroffenen ist die Möglichkeit einzuräumen, Widerspruch gegen die Einsicht in patientenbezogene Informationen aus Vorsorgemaßnahmen zu erheben (Art. 21 DSGVO). Mit Blick auf das in § 2 Abs. 1 Nr. 3 ArbMedVV bestehende Recht des Beschäftigten, Untersuchungen abzulehnen, gilt für die Informationserhebung durch Einsicht in die gesundheitsbezogene Dokumentation früherer Untersuchungen nichts anderes. Eine Löschung dieser Informationen aus Anlass des Arztwechsels kommt im Hinblick auf die zehnjährige und evtl. längere Aufbewahrungsfrist ärztlicher Unterlagen (s. o. 4.) nicht in Betracht. Die gesperrten Unterlagen dürfen nicht vom neuen Betriebsarzt beigezogen werden; sie sind besonders geschützt im Betrieb aufzubewahren, bis die Löschungsfrist erreicht ist. Die Verwahrung im Betrieb unter Verschluss durch den amtierenden Betriebsarzt ist auch aus praktischer Sicht sachgerecht, da sich ein Beschäftigter nach Verlassen des Unternehmens bei Bedarf eher an den früheren Arbeitgeber wenden wird als an einen gegebenenfalls extern beauftragten Betriebsarzt.[26]

Um den Pflichten nach dem ASiG und der Verordnung zur arbeitsmedizinischen Vorsorge (ArbMedVV) entsprechen zu können, muss ein Zugriff auf bestimmte Daten des Vorgängers möglich sein. Das gilt für die für die arbeitsmedizinische Tätigkeit erforderlichen Stammdaten der Beschäftigten und die Angaben, die gegenüber dem Arbeitgeber zu attestieren sind, also Art und Datum der Vorsorge sowie Datum der nächsten Vorsorge. Auch die vom Betriebsarzt erstellte Arbeitsplatzbeschreibung steht im Zugriff des Nachfolgers. Es macht dabei keinen Unterschied, ob die Dokumentation analog oder digital geführt wird. Bei elektronischer Aktenführung können die Zugriffsmöglichkeiten durch entsprechende Rechtevergabe gesteuert werden.

Beim Wechsel eines internen Betriebsarztes verbleiben die patientenbezogenen Unterlagen im Eigentum und in der datenschutzrechtlichen Verantwortlichkeit des Arbeitgebers. Wegen des Patientengeheimnisses darf der Arbeitgeber aber keinen Einblick in die Unterlagen nehmen. Er hat sie vielmehr dem neu bestellten Betriebsarzt zur Verfügung zu stellen.

Beim Wechsel von externen Betriebsärzten sollte der frühere Betriebsarzt seine Dokumentation unmittelbar an seinen Nachfolger übergeben, zu dessen Bestellung der Arbeitgeber gesetzlich verpflichtet ist. Auf diese Weise kommt der scheidende Betriebsarzt auch seiner Verpflichtung aus § 10 Abs. 4 MBOÄ nach, dafür Sorge zu tragen, dass seine ärztlichen Aufzeichnungen in gehörige Obhut gegeben werden.

Der ausscheidende Betriebsarzt hat kein Recht, die von ihm erstellten Unterlagen „mitzunehmen". Diese sind in Ausübung der gesetzlichen Pflicht nach dem ASiG entstanden. Sie verlieren durch den Wechsel nicht ihre Funktion gemäß § 3 ASiG. Insofern besteht ein Unterschied zu Unterlagen, die im Bereich sonstiger ärztlicher Praxen entstehen.

Verantwortlicher im Sinne des Datenschutzrechts bleibt im Falle des internen Betriebsarztes der Betrieb des Arbeitgebers. Im Fall des externen Betriebsarztes ist dieser bei einem Wechsel gemäß dem ASiG verpflichtet, die Dokumentation an den übernehmenden externen Betriebsarzt oder an den Arbeitgeber

zu übergeben. Dem ausscheidenden Betriebsarzt kann und muss unter Umständen, z. B. zum Zweck der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (vgl. Art. 9 Abs. 2 lit. f DSGVO), Zugriff auf insofern erforderliche Daten eingeräumt werden.

Für Beschäftigte, die ihre Betroffenenrechte (Art. 12 ff. DSGVO, § 630g BGB) wahrnehmen wollen, besteht so weiterhin die Möglichkeit, diese gegenüber ihrem (früheren) Arbeitgeber auszuüben. Dieser muss dann über den jeweiligen Betriebsarzt dafür sorgen, dass die entsprechenden patientenbezogenen Unterlagen dem nachfragenden betroffenen Arbeitnehmer offenbart werden.

Die dargestellte Vorgehensweise entspricht dem sog. „Zwei-Schrank-Modell", das auch außerhalb des betriebsärztlichen Bereichs für den Wechsel eines Arztes in einer Praxis und die Übergabe der bisherigen Dokumentation an seinen Nachfolger anzuwenden ist.[27] Der abgebende Arzt behält dabei grundsätzlich eine informationsrechtliche Verfügungsbefugnis an den Altakten und übergibt sie in einem verschlossenen Schrank dem Nachfolger, der sich wiederum im Übernahmevertrag speziell verpflichtet, den Datenbestand zu verwahren und fallbezogen Zugriff auf einzelne Akten bzw. Datensätze zu nehmen, wenn eine frühere Patientin oder ein früherer Patient ihn aufsucht. Erfolgt dies, so führt der übernehmende Arzt die Dokumentation in eigener Verantwortung fort. Die alte Akte darf dann bei einem entsprechenden Einverständnis dieses Patienten entnommen und durch den Nachfolger mit der laufenden Patientendokumentation des Erwerbers zusammengeführt werden. Das Einverständnis ist in der Akte zu dokumentieren. Dies bedeutet, dass für den Nachfolger die datenschutzrechtliche Verfügungsbefugnis über die Akten nur eingeschränkt besteht, unabhängig davon, ob bzw. für welchen Zeitpunkt ein sachenrechtlicher Eigentumsübergang verabredet wird.[28] Bei diesem Modell wird also unterschieden zwischen der Übertragung des Gewahrsams an dem Gesamtaktenbestand und der daten- bzw. patientenschutzrechtlich wesentlich sensibleren konkreten Einsichtnahme. Bei elektronisch geführten Patientendaten ist der alte Bestand zu sperren und der Zugriff hierauf z. B. mittels Passwort zu sichern.

Für einen erstmaligen Zugriff auf einen Patientendatensatz durch den Praxisnachfolger ist die Zustimmung des Patienten erforderlich. Liegt diese vor, so darf insoweit der Datensatz vom Nachfolger freigeschaltet und weitergenutzt werden. Es wird davon ausgegangen, dass die Einwilligung eines Patienten in die Übernahme durch einen Nachfolger die gesamte Patientenakte umfasst. Bringt ein Patient jedoch zum Ausdruck, dass nur Teile der Akte bzw. der Unterlagen übernommen werden sollen, so muss dieser Wunsch berücksichtigt werden (vgl. § 9 Abs. 4 MBOÄ).[29]

Um Probleme bei der Aktenübergabe bei Aufgabe der Tätigkeit als externer Betriebsarzt zu umgehen, empfiehlt sich eine vertragliche Vereinbarung mit dem Unternehmen des Arbeitgebers, dass die Altakten entsprechend dem „Zwei-Schrank-Modell" an den Nachfolger übergeben werden.[30]

1 Weichert in Kühling/Buchner, DS-GVO – BDSG, Kommentar, 2. Aufl. 2018, Art. 9 Rn. 138 ff.

2 Weichert, DuD 2017, 541.

3 Gesetz v. 30.06.2017, BGBl. I S. 2097.

4 Weichert, DuD 2017, 542.

5 Washausen in Kingreen/Kühling, Gesundheitsdatenschutzrecht, 2015, S. 411 ff.

6 Wedde in Däubler/Wedde/Weichert/Sommer, EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, Art. 88 Rn. 1; Maschmann in Kühling/Buchner (En. 1), Art. 88 Rn. 1 7 ff., 19.

7 Weichert in Däubler u. a. (En. 6), Art. 4 Rn. 88; Hartung in Kühling/Buchner (En. 1), Art. 4 Nr. 7 Rn. 9.

8 EuGH 05.06.2018 – C-210/16, Rn. 38, NZA 2018, 921.

9 Weichert in Kühling/Buchner (En. 1), Art. 9 Rn. 112 f.; Weichert RDV 2007, 189.

10 Brunhöber in Aufhauser/Brunhöber/Igl, Arbeitssicherheitsgesetz, 4. Aufl. 2010, § 2 Rn. 2.

11 Weichert RDV 2007, 191; Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Gesundheitsdaten im Arbeitsverhältnis, 31.03.2014, https://www.datenschutzzentrum.de/artikel/193-Gesundheitsdaten-im-Arbeitsverhaeltnis.html, III. zu undifferenziert Washausen in Kingreen/Kühling (En. 5), S. 420.

12 Weidenkaff in Palandt, Bürgerliches Gesetzbuch, 78. Aufl. 2019, § 630a Rn. 5.

13 Washausen in Kingreen/Kühling (En. 5), S. 424-427.

14 ArbMedVV v. 18.12.2008, BGBl. I S. 2768, zuletzt geändert am 15.11.2016, BGBl. I S. 2549.

15 Washausen in Kingreen/Kühling (En. 5), S. 425; Weichert RDV 2007, 192 f. mit Angabe von weiteren Vorsorgepflichten, Pieper, ArbSchR, 6. Aufl. 2017, Arbeitssicherheitsgesetz Rn. 80-87; vgl. Däubler, Gläserne Belegschaften, 8. Aufl. 2019, Rn. 276 f.

16 Washausen in Kingreen/Kühling (En. 5), S. 424 f.

17 GMBl Nr. 5, 24.02.2014, S. 90.

18 ULD (En. 11), III.

19 Däubler (En. 15), Rn. 282.

20 Hinweis des Verband Deutscher Betriebs- und Werkärzte (VDBW), Hinweise zur datenschutzgerechten Übergabe der Patientenakten beim Wechsel von Betriebsärzten, VDBW aktuell, April 2019, S. 40.

21 Aufhauser in Aufhauser u. a. (En. 10), § 8 Rn. 3.

22 Z. B. § 15 SGB VII, § 202 SGB VII i. V. m. § 5 BKVO, Däubler (En. 15), Rn. 272a.

23 Weichert, RDV 2007, 191; vgl. ULD (En. 11), III.

24 Washausen in Kingreen/Kühling (En. 5), S. 425.

25 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Hinweise zur datenschutzgerechten Übergabe einer Arztpraxis mit Patientenakten und zum Wechsel von Betriebsärzten, 10.01.2015/10.04.2015, https://www.datenschutzzentrum.de/artikel/47-Hinweise-zur-datenschutzgerechten-UEbergabe-einer-Arztpraxis-mit-Patientenakten-und-zum-Wechsel-von-Betriebsaerzten.html, 2.

26 VDBW (En. 20), S. 41.

27 Weichert RDV 2007, 191; ULD, Praxisüber- oder -aufgabe, https://www.datenschutzzentrum.de/medizin-soziales/faq/arztpraxis/#20.

28 VDBW (En. 20), S. 42.

29 ULD (En. 25), 1.; Rehborn in Prütting, Medizinrecht, 3. Aufl. 2014, § 9 MBOÄ Rn. 9 m. w. N.

30 ULD (En. 25), 2.; VDBW (En. 20), S. 42.

Werner Hülsmann

Datenschutzrechtliche Aspekte der Verarbeitung von Gesundheits- und Sozialdaten bei Personenschäden durch Sozialversicherungen und in Regress genommene Haftpflichtversicherungen

Bei Unfällen mit Personenschäden, die durch Dritte verursacht werden, übernimmt gewöhnlich die entsprechende Sozialversicherung der geschädigten Person (Gesetzliche Krankenkasse, Unfallversicherung, Berufsgenossenschaft) erst einmal die Behandlungskosten, nimmt aber dann die Haftpflichtversicherung der den Unfall verursachenden Person in Regress. Die Haftpflichtversicherungen wiederum nehmen für die Bearbeitung bzw. Abwehr dieser Regressforderungen häufig Dienstleister in Anspruch. Die Rechtsgrundlagen für die damit verbundenen Datenverarbeitungen und Datenweitergaben werden in diesem Artikel[1] erörtert.

1. Einleitung

Für die Verarbeitung personenbezogener Daten (im Folgenden: „Daten“) gilt ein sogenanntes Verbot mit Erlaubnisvorbehalt. Dies bedeutet, dass der Verantwortliche[2] für jede Verarbeitung personenbezogener Daten eine Erlaubnis benötigt. Ein wichtiger Hinweis sei hier erlaubt: Die Einwilligung der betroffenen Person ist nur eine von mehreren Möglichkeiten für eine Erlaubnis. Die Erlaubnisse für die Verarbeitung von personenbezogenen Daten sind für die hier zu betrachtenden Institutionen und Unternehmen grundsätzlich im Art. 6 Abs. 1 der EU-Datenschutz-Grundverordnung (DSGVO) geregelt. Erlaubt sind danach Datenverarbeitungen

a) auf Grund der wirksamen Einwilligung der betroffenen Personen,
b) zur Anbahnung oder Erfüllung eines Vertrags mit der betroffenen Person,
c) zur Erfüllung gesetzlicher Verpflichtungen,
d) „um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen“,
e) soweit sie erforderlich für die Wahrnehmung einer Aufgabe sind, „die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde“ oder
f) auf der Basis einer Abwägung der Interessen von Verantwortlichen und den von der Verarbeitung betroffenen Personen.

2. Verarbeitung von personenbezogenen Gesundheitsdaten

Bei der Verarbeitung personenbezogener Daten im Zusammenhang mit der Regulierung von Personenschäden sind allerdings bestimmte Besonderheiten zu beachten. Zum einen handelt es sich bei diesen Daten um Sozialdaten im Sinne des § 67 Abs. 2 Sozialgesetzbuch (SGB) X, die gemäß Art 35 SGB I dem Sozialgeheimnis unterliegen. Zum anderen handelt es sich auch um Gesundheitsdaten, die gemäß Art. 9 Abs. 1 DSGVO zu den besonderen Kategorien personenbezogener Daten gehören und deren Verarbeitung in Art. 9 Abs. 1 DSGVO untersagt wird. Von diesem Verbot gibt es allerdings auch Ausnahmen. So regelt Art. 9 Abs. 2 DSGVO:

„Absatz 1 gilt nicht in folgenden Fällen:

a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,
b) die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist,
c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben,
d) die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden,
e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,
f) die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich,

g) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich,
h) die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich,
i) die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich, oder
j) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 erforderlich.“[3]

Zu den in Buchstabe h) genannten Zwecken dürfen die Daten nur von Fachpersonal, das einem Berufsgeheimnis nach nationalem Recht unterliegt (wie z.B. das Patientengeheimnis) oder unter der Verantwortung derartigen Fachpersonals verarbeitet werden.[4] Die Nationalstaaten dürfen gemäß Art. 9 Abs. 4 DSGVO „zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist.“ Somit sind die in den SGB enthaltenen besonderen Regelungen zum Umgang mit Sozialdaten, soweit sie Gesundheitsdaten sind, auch nach dem Wirksamwerden der DSGVO zulässig.

Ein weiterer wesentlicher Aspekt bei der Verarbeitung von Gesundheitsdaten ist der Umstand, dass als Rechtsgrundlage und damit als Erlaubnis für die Verarbeitung von Gesundheitsdaten nur und ausschließlich die in Art. 9 Abs. 2 DSGVO genannten Ausnahmen bzw. die aufgrund von Art. 9 Abs. 4 DSGVO in nationalen Gesetzen geregelten Ausnahmen herangezogen werden dürfen. Somit sind die Erlaubnisse aus Art. 6 Abs. 1 DSGVO allein für Gesundheitsdaten nicht nutzbar.[5] Damit fällt auch die – für „normale“ personenbezogene Daten mögliche – Interessenabwägung aus Art. 6 Abs. 1 Buchst. f) DSGVO als Erlaubnis zur Verarbeitung besonderer Kategorien personenbezogener Daten und damit zur Verarbeitung von Gesundheitsdaten weg.

Des Weiteren ist zu beachten, dass Sozialdaten gemäß § 78 SGB X auch dann noch einem besonderen Schutz unterliegen, wenn sie – wie es bei Regressansprüchen regelmäßig geschieht – von Sozialversicherungsträgern an Stellen übermittelt werden, die nicht dem Sozialgeheimnis aus § 35 SB I unterliegen. So heißt es in § 78 SGB X Abs. 1 Sätze 1 bis 3:

„Personen oder Stellen, die nicht in § 35 des Ersten Buches genannt und denen Sozialdaten übermittelt worden sind, dürfen diese nur zu dem Zweck verarbeiten, zu dem sie ihnen befugt übermittelt worden sind. Eine Übermittlung von Sozialdaten nach den §§ 68 bis 77 oder nach einer anderen Rechtsvorschrift in diesem Gesetzbuch an eine nicht-öffentliche Stelle auf deren Ersuchen hin ist nur zulässig, wenn diese sich gegenüber der übermittelnden Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dem sie ihr übermittelt werden. Die Dritten haben die Daten in demselben Umfang geheim zu halten wie die in § 35 des Ersten Buches genannten Stellen.“

3. Formen der Weitergabe von personenbezogenen Daten

Während das alte Bundesdatenschutzgesetz (BDSG) nur zwei Formen der Datenweitergabe im Zusammenhang mit einer Dienstleistungserbringung kannte, nämlich die Auftragsdatenverarbeitung (wie die Auftragsverarbeitung im alten Datenschutzrecht hieß) und die Datenübermittlung (im Rahmen einer sogenannten Funktionsübertragung), kennt die DSGVO auch noch das Konstrukt der gemeinsamen Verantwortlichen. Alle drei Formen werden im Folgenden kurz dargestellt. Auf die Auftragsverarbeitung (AV) wird anschließend näher eingegangen.

3.1. Funktionsübertragung

Für den Begriff der sogenannten Funktionsübertragung gab und gibt es keine Legaldefinition. Auch in den alten Datenschutzgesetzen kam dieser Begriff nicht vor. Allerdings wurde und wird der Begriff „Funktionsübertragung“ in der juristischen Fachliteratur u.a. dazu verwendet, um die Datenübermittlung zum Zwecke der Beauftragung einer mehr oder weniger konkreten Dienstleistung von anderen Datenübermittlungen (wie sie z.B. im Bereich des Adresshandels erfolgen) zu unterscheiden. In der Begründung zum „Entwurf eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes“ der Bundesregierung aus dem Jahre 1989 wird der Begriff „Funktionsübertragung“ in Abgrenzung zur Auftragsdatenverarbeitung genannt:

„Wie bisher handelt es sich nicht um Auftragsdatenverarbeitung im Sinne dieser Vorschrift, wenn neben der Datenverarbeitung auch die zugrundeliegende Aufgabe übertragen wird (Funktionsübertragung). In diesem Falle hat derjenige, dem die Funktion übertragen wird, alle datenschutzrechtlichen Pflichten, insbesondere die Ansprüche des Betroffenen, zu erfüllen.“[6]

In dieser Bedeutung gibt es die Funktionsübertragung nach wie vor, auch die DSGVO hat nichts daran geändert.

Im Falle einer Datenübermittlung im Rahmen einer „Funktionsübertragung“ muss der abgebende Verantwortliche eine Rechtsgrundlage, also eine Erlaubnis, für diese Datenübermittlung haben. Die empfangende Stelle (Institution oder Firma) muss selbst eine eigenständige Erlaubnis für die Verarbeitung der erhaltenen Daten haben. Die empfangende Stelle muss zudem alle datenschutzrechtlichen Pflichten, die für Verantwortliche im Sinne des Art. 4 Ziff. 7 DSGVO gelten, erfüllen.

3.2. Gemeinsame Verantwortliche

Im alten BDSG war das Konstrukt der gemeinsamen Verantwortlichen nicht enthalten. Unter der DSGVO ist dieses Konstrukt EU-weit nutzbar:

„Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.“[7]

Hier müssen alle beteiligten Verantwortlichen eine Rechtsgrundlage, also eine Erlaubnis zur Verarbeitung der personenbezogenen Daten haben. Es reicht hier keinesfalls aus, dass nur einer der Verantwortlichen eine Erlaubnis für die Verarbeitung personenbezogener Daten nachweisen kann.

3.3. Auftragsverarbeitung

Grundsätzlich hat sich am Konstrukt der Auftragsdatenverarbeitung, wie die Auftragsverarbeitung im alten Datenschutzrecht hieß, nicht viel geändert. Der Auftraggeber (jetzt: der Verantwortliche) bleibt auch nach der DSGVO für die Verarbeitung der personenbezogenen Daten beim Auftragnehmer (jetzt: der Auftragsverarbeiter) verantwortlich. Der Auftragsverarbeiter ist in erster Linie nur dafür verantwortlich, die vom Verantwortlichen erhaltenen Daten im Rahmen der Auftragsverarbeitung nur entsprechend des konkreten Auftrags und eventueller ergänzender Weisungen des Verantwortlichen und damit auch nur zu dessen Zwecken zu verarbeiten. Eine Verarbeitung zu eigenen Zwecken des Auftragsverarbeiters ist im Rahmen der Auftragsverarbeitung unzulässig.

Auf der anderen Seite benötigt der Auftragsverarbeiter keine eigene Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten, die er vom Verantwortlichen zur Erfüllung des Auftrags erhält. Der Auftragsverarbeiter zählt im Rahmen der Auftragsverarbeitung nicht als Dritter gegenüber dem Verantwortlichen. Sofern also der Verantwortliche die personenbezogenen Daten verarbeiten darf, darf er diese personenbezogenen Daten auch an einen Auftragsverarbeiter weitergeben, der diese Daten dann – aber nur und ausschließlich zur Erfüllung des Auftrags – auf Basis des Auftrags und auf Basis der Verarbeitungserlaubnis, auf die sich der Verantwortliche berufen kann, verarbeiten darf. Dies gilt allerdings nur, wenn die in Art. 28 DSGVO an die Auftragsverarbeitung gestellten Anforderungen sowohl auf Seiten des Verantwortlichen als auch auf Seiten des Auftragsverarbeiters erfüllt werden. Für die Beauftragung von Auftragsverarbeitern durch Sozialversicherungsträger ist ergänzend zu Art. 28 DSGVO noch § 80 SGB 10 zu beachten. So müssen Sozialversicherungsträger ihre Rechts- oder Fachaufsicht „rechtzeitig vor der Auftragserteilung“ über diese informieren. Eine Beauftragung von nichtöffentlichen Stellen ist nur zulässig,

„wenn

1. *beim Verantwortlichen sonst Störungen im Betriebsablauf auftreten können oder*
2. *die übertragenen Arbeiten beim Auftragsverarbeiter erheblich kostengünstiger besorgt werden können.“* (§ 80 Abs. 3 SGB X)

Ausgenommen hiervon sind nur „die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen“ durch nichtöffentliche Stellen.

4. Rechtliche Anforderungen an die Auftragsverarbeitung

Eine wesentliche Anforderung an die Auftragsverarbeitung ist, dass der Verantwortliche die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten bestimmt. Eine Bestimmung der Mittel durch den Verantwortlichen ist allerdings auch dann gegeben, wenn der Auftragsverarbeiter nur seine bereits vorhandenen Mittel (Infrastruktur, Server, etc.) anbietet, da bereits durch die Auswahl des Auftragsverarbeiters in diesem Fall die Mittelbestimmung erfolgt. Art. 28 Abs. 10 DSGVO sagt ausdrücklich:

„Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.“[8]

Weitere Anforderungen an eine datenschutzkonforme Auftragsdatenverarbeitung sind:

- Sorgfältige Auswahl des Auftragsverarbeiters – So muss der Auftragsverarbeiter nachweisen können, dass er die gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen durchführt, so dass „die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.“[9]
- Einsatz von Subunternehmern (Unterauftragsverarbeitern) nur mit schriftlicher Genehmigung des Verantwortlichen.
- Die Auftragsverarbeitung erfolgt auf der Basis eines Vertrags (AV-Vertrag, schriftlich oder in elektronischer Form) zwischen Verantwortlichen und Auftragsverarbeiter. In diesem Vertrag sind festzulegen:
  - Gegenstand und Dauer der Verarbeitung,
  - Art und Zweck der Verarbeitung,
  - die Art der personenbezogenen Daten,
  - die Kategorien betroffener Personen und
  - die Pflichten und Rechte des Verantwortlichen.

- Der Auftragsverarbeiter darf „die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen“[10] verarbeiten.
- Der Auftragsverarbeiter „gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen“.[11]
- Der Auftragsverarbeiter muss sicherstellen, dass er „nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt und die vorhandenen Kopien löscht.“[12]

Eine Verarbeitung der vom Verantwortlichen oder in dessen Auftrag erhaltenen personenbezogenen Daten für eigene Zwecke des Auftragsverarbeiters ist im Rahmen der Auftragsverarbeitung nicht zulässig. Eine Zusammenführung von Daten unterschiedlicher Verantwortlicher (Auftraggeber) ist im Rahmen einer Auftragsverarbeitung auch dann unzulässig, wenn eine solche Zusammenführung der Erfüllung der einzelnen Aufträge dienlich wäre. Eine derartige Zusammenführung wäre nur dann datenschutzrechtlich zulässig, wenn die verschiedenen Auftraggeber eine Rechtsgrundlage für die Übermittlung der Daten an alle anderen Verantwortlichen hätten oder als gemeinsam Verantwortliche im Sinne des Art. 26 DSGVO (s.o.) agieren würden. Hierzu wäre es aber erforderlich, dass seitens der Verantwortlichen ein Erlaubnistatbestand für die gemeinsam verantwortliche Verarbeitung und insbesondere für das Zusammenführen ihrer Daten vorliegt. Im Bereich der Verarbeitung von Gesundheits- und Sozialdaten kann aber grundsätzlich davon ausgegangen werden, dass derartige Erlaubnistatbestände nicht vorliegen.

4.1. Auftragsverarbeitung und Berufsgeheimnisse

Zur Vollständigkeit erfolgt an dieser Stelle noch ein kurzer Hinweis auf die Berufsgeheimnisse aus § 203 Strafgesetzbuch (StGB): Lange Zeit war es strittig, ob die Beauftragung eines Dienstleisters im Rahmen der Auftragsverarbeitung eine unbefugte Offenbarung von Daten, die einem Berufsgeheimnis unterliegen, darstellt oder nicht. Durch die aktuelle Formulierung von § 203 Abs. 3 StGB ist klargestellt, dass auch für Daten, die einem Berufsgeheimnis unterliegen, eine den Anforderungen des Art. 28 DSGVO genügende Auftragsverarbeitung keine unbefugte Offenbarung darstellt und somit zulässig ist, ohne dass von den betroffenen Personen eine Schweigepflichtentbindung erforderlich wäre. Allerdings muss sichergestellt sein, dass der Dienstleister (Auftragsverarbeiter) nur auf die dem Berufsgeheimnis unterliegenden Daten zugreifen kann, die er für die Erbringung der Dienstleistung zwingend benötigt.

5. Fazit

Die Auftragsverarbeitung ist auch im Bereich der Verarbeitung von Gesundheits- und Sozialdaten eine datenschutzrechtlich zulässige Möglichkeit, sofern der Verantwortliche diese Gesundheitsdaten zu eigenen Zwecken gemäß Art. 9 Abs. 2 DSGVO oder gemäß bereichsspezifischer Gesetze, wie beispielsweise den Sozialgesetzbüchern, verarbeiten darf, der Auftragsverarbeiter die Daten nur zu den Zwecken zu denen er sie erhalten hat und nur für den jeweiligen Verantwortlichen verarbeitet und im Übrigen die oben genannten Bedingungen eingehalten werden.

1 Dieser Artikel ist eine überarbeitete Fassung von Teil 1 der Erstveröffentlichung in: Huber, Kornes, Mathis, Thoennеßen (Hrsg.): Fachtagung Personenschaden, Nomos Verlagsgesellschaft, Seiten 97 - 106

2 Laut Art. 4 Ziff. 7 DSGVO bezeichnet „'Verantwortlicher' die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;", also das Unternehmen oder die Institution, in dessen oder deren Verantwortung die Verarbeitung personenbezogener Daten erfolgt. Hierzu gehören im hiesigen Zusammenhang zumindest die Sozialleistungsträger ebenso wie die Haftpflichtversicherungen.

3 Art. 9 Abs. 2 DSGVO

4 vgl. Art. 3 Abs. 9 DSGVO

5 Dies ergibt sich zum einen aus der strikten Untersagung aus Art. 9 Abs. 1 DSGVO und zum anderen daraus, dass die Einwilligung der betroffenen Person als Ausnahme der Untersagung in Art. 9 Abs. 2 Buchst. a) DSGVO ausdrücklich genannt ist. Bei einer alleinigen Anwendbarkeit von Art. 6 Abs. 1 DSGVO wäre dies nicht erforderlich gewesen.

6 BT-Drucksache Nr. 11/4306 vom 06.04.1989, S. 43, online verfügbar unter https://dipbt.bundestag.de/doc/btd/11/043/1104306.pdf, abgerufen am 02.10.2019

7 Art. 26 Abs. 1 DSGVO

8 Die Art. 82 bis 84 DSGVO regeln „Haftung und Recht auf Schadenersatz", „Allgemeine Bedingungen für die Verhängung von Geldbußen" und „Sanktionen".

9 Art. 28 Abs. 1 DSGVO

10 Art. 28 Abs. 3 Buchst. a) DSGVO

11 Art. 28 Abs. 3 Buchst. b) DSGVO

12 Art. 28 Abs. 3 Buchst. b) DSGVO

Werner Hülsmann

Sammlung, Auswertung und Verarbeitung von Gesundheitsdaten durch die Haftpflichtversicherer über ihre Dienstleister am Beispiel ACTINEO: Datenschutzkonformität vor dem Hintergrund des Rechts auf informationelle Selbstbestimmung und der DSGVO

1. Einleitung

In diesem Artikel[1] geht es in erster Linie um eine Betrachtung der Aktivitäten der Sammlung, Auswertung und Verarbeitung von Gesundheitsdaten durch die Haftpflichtversicherungen und durch deren beauftragte Dienstleister am Beispiel des Dienstleisters ACTINEO GmbH (im Folgenden ACTINEO) aus Sicht der betroffenen Personen, also aus Sicht der geschädigten Personen, die aufgrund eines durch eine oder einen Dritten verursachten Personenschadensfalles eine medizinische Behandlung benötigen. Hierbei werden die Leistungen im Regelfall erst einmal von den Sozialversicherungsträgern (insbesondere Krankenversicherung, Rentenversicherung, gesetzliche Unfallversicherung) übernommen und dann mit der Haftpflichtversicherung des Schädigers abgerechnet.

Der als Beispiel ausgewählte Dienstleister ist zwar nicht der einzige, scheint aber doch der am weitesten verbreitete Dienstleister zu sein, der von den Haftpflichtversicherungen beauftragt wird, um die ihnen im Rahmen der Regulierung von Haftpflichtschäden von den Sozialversicherungsträgern gestellten Abrechnungen zu prüfen[2].

ACTINEO bezeichnet sich selbst als „der deutsche Marktführer für die Digitalisierung und medizinische Einschätzung von Personenschäden“.[3]

„Zu den Leistungen von ACTINEO bei der Personenschadenregulierung gehören unter anderem

- die Beschaffung, Strukturierung und Plausibilisierung medizinischer Daten,
- die Normierung und Digitalisierung von Personenschäden,
- die Entwicklung und der Aufbau von Prädiktionsmodellen und KI-Lösungen im Personenschaden,
- die Prozessautomatisierung sowie digitale Instrumente für die Steuerung und das Controlling im Personenschaden,
- die systematische und medizinisch fundierte Rechnungsprüfung,
- die Einschätzung und Erstellung medizinischer Gutachten, Pflegegutachten und Überleitungsmanagement sowie
- ein toolgestütztes medizinisches Vor-Ort-Assessment.“[4]

Bereits aus dieser kurzgefassten Leistungsbeschreibung wird deutlich, dass hier wesentlich mehr Dienstleistungen angeboten werden, als im Rahmen einer Auftragsverarbeitung im Sinne des Art. 28 DSGVO erbracht werden können. Vielmehr verarbeitet ATINEO offensichtlich einen Großteil der Schadensdaten zu eigenen Zwecken, wie z.B. zum Zwecke einer systematischen und medizinisch fundierten Rechnungsprüfung. Eine medizinisch fundierte Rechnungsprüfung kann nicht als Auftragsverarbeitung angeboten werden, da eine solche weit über die eigentliche Datenverarbeitung hinausgeht. Auch die Entwicklung und der Aufbau von Prädiktionsmodellen und KI-Lösungen im Bereich Personenschaden lässt sich nicht als Auftragsverarbeitung darstellen.

Aus datenschutzrechtlicher Sicht geht es bei den personenbezogenen Daten, die zur Abrechnung von Personenschadensfällen anfallen, um Sozialdaten und um Gesundheitsdaten. Des Weiteren ist § 203 Strafgesetzbuch (StGB) „Verletzung von Privatgeheimnissen“ zu beachten. Eine Darstellung der formalen datenschutzrechtlichen Zulässigkeit findet sich im vorgehenden Artikel in dieser Ausgabe[5].

2. Die Gesundheit und die „Gesundheitswirtschaft“

Wer sich intensiver mit dem Gesundheitssystem beschäftigt, wird unweigerlich auf einen Begriff stoßen: „Gesundheitswirtschaft“. Das Bundesministerium für Wirtschaft und Energie (BMWi) veröffentlicht immer wieder Pressemitteilungen, in denen es um die „Gesundheitswirtschaft“ geht[6]. Wohlgemerkt, nicht das Bundesministerium für Gesundheit, sondern das Bundesministerium, das für die Wirtschaft zuständig ist. Interessant ist in diesem Zusammenhang auch der Branchenfokus „Gesundheitswirtschaft“ des BMWi.[7]

Eigentlich sollte es bei der Gesundheit um den Menschen gehen und nicht um wirtschaftliche Aspekte. Gesundheit sollte kein Gut sein, das Renditeanforderungen unterliegt. Sicher ist es wünschenswert, wenn unser Gesundheitssystem effizient und wirtschaftlich funktioniert, also unter anderem unnötige Kosten vermieden werden, Heilmittel eingesetzt werden, die für die Heilung förderlich sind. Aber genau hier stellen sich die Fragen: Wer entscheidet, welche Kosten im konkreten Einzelfall nötig oder unnötig sind? Wer entscheidet, welche Heilmittel im konkreten Einzelfall für die Heilung förderlich sind? Sollten diese Entscheidungen nicht unter den gesellschaftlich und politisch gewollten Rahmenbedingungen zwischen Arzt oder Ärztin und Patient oder Patientin geklärt werden?

Alleine der Begriff „Gesundheitswirtschaft" degradiert den Menschen, insbesondere den kranken Menschen zur Ware, zum bloßen Objekt. Aber auch die Personen, die die medizinische Leistung erbringen, die Ärztinnen und Ärzte, Krankenschwestern und Krankenpfleger, Therapeutinnen und Therapeuten werden durch den Begriff der „Gesundheitswirtschaft" zur Ware, zum Objekt degradiert. Dabei sollte doch der Mensch im Mittelpunkt des Gesundheitssystems stehen.

In einer vermutlich 2015 erstellten Präsentation, die von einer Mitarbeiterin einer gesetzlichen Krankenversicherung erstellt wurde, findet sich die Aussage:

„Ca. 20 Prozent der Versicherten verursachen ca. 80 Prozent der Kosten …

… und etwa 80% der Kosten entstehen in den letzten beiden Lebensjahren".[8]

An dieser Stelle seien die unter dem Aspekt einer renditeorientierten „Gesundheitswirtschaft" möglichen Schlussfolgerungen und Gedankenexperimente der geneigten Leserin und dem geneigten Leser überlassen. Aber Vorsicht: Es könnte makaber werden.

3. Datenschutz und das Recht auf informationelle Selbstbestimmung

3.1. Datenschutz ist ein Grundrecht

Bereits in der Charta der Grundrechte der Europäischen Union (2010/C 83/02, EU-Grundrechtecharta) von 2010 wird postuliert:

„Artikel 7
Achtung des Privat- und Familienlebens

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

Artikel 8
Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht."

Die DSGVO setzt dies um und „schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten" (vgl. Art. 1 Abs. 2 DSGVO). Es geht beim Datenschutz also immer um den Schutz der Grundrechte der Personen, deren Daten verarbeitet werden.

Erwägungsgrund (EWG) 4 Satz 1 fordert:
„Die Verarbeitung personenbezogener Daten sollte im Dienste der Menschheit stehen."

Die englische Version wird da noch deutlicher:
„The processing of personal data should be designed to serve mankind."
(zu Deutsch etwa: „Die Verarbeitung personenbezogener Daten sollte so gestaltet/entworfen werden, dass sie der Menschheit dient.")

Das ist ein hehres, aber leider auch ein sehr abstraktes Ziel. Der Umsetzung und Konkretisierung dieses Ziels dienen unter anderem die in Art. 5 Abs. 1 DSGVO festgelegten sechs Grundsätze der Datenverarbeitung. Die Schlagwörter dieser sechs Grundsätze lauten:

a) *„Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz"*
b) *„Zweckbindung"*
c) *„Datenminimierung"*
d) *„Richtigkeit"*
e) *„Speicherbegrenzung"*
f) *„Integrität und Vertraulichkeit"*

3.2. Das Recht auf informationelle Selbstbestimmung

Älter als die EU-Grundrechtecharta ist das sogenannte Volkszählungsurteil des Bundesverfassungsgerichts (BVerfG) vom 15.12.1983 (BVerfGE 65, 1-71[9]), in dem das Recht auf informationelle Selbstbestimmung aus Art. 1 Abs 1 und Art. 2 Abs. 1 Grundgesetz (GG) abgeleitet wird. Dort heißt es im ersten Leitsatz:

„Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."[10]

Das Bundesverfassungsgericht führt in seiner Begründung aus
„Individuelle Selbstbestimmung setzt aber – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, dass dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß."[11]

Und weiter:

„Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art 2 Abs. 1 in Verbindung mit Art 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."[12]

Zur Nutzung von personenbezogenen Daten zu statistischen Zwecken führt das BVerfG aus:

„Es müssen klar definierte Verarbeitungsvoraussetzungen geschaffen werden, die sicherstellen, dass der Einzelne unter den Bedingungen einer automatischen Erhebung und Verarbeitung der seine Person betreffenden Angaben nicht zum bloßen Informationsobjekt wird.“[13]

3.3. Der Mensch als Individuum

Aus den beiden vorherigen Abschnitten wird deutlich, dass der Mensch auch in der modernen Informationsgesellschaft immer als Individuum, als Subjekt gesehen werden muss und nie als bloßes Objekt, das auf seine Daten reduziert wird, gesehen werden darf.

4. Datensammlung durch die Haftpflichtversicherungen und ihren Dienstleister ACTINEO

ACTINEO wirbt auf ihrer Website mit dem Spruch:

„Wir tun mehr, weil am Ende der Nutzen zählt.“[14]

Die Frage ist nur, Nutzen für wen? Bei weiterer Sichtung der Website wird sehr schnell deutlich, dass es hier nicht um den Nutzen für die geschädigte Person geht, sondern um den Nutzen für den Kunden von ACTINEO, der Haftpflichtversicherung, die von einer Sozialversicherung bezüglich der Übernahme der Leistungen in einem Personenschaden-Haftpflichtfall in Regress genommen wird.

So schreibt ACTINEO:

„Seit 2009 stehen wir für Innovation und Kostenoptimierung im Personenschaden. Inzwischen sind wir der deutsche Marktführer für die Digitalisierung und medizinische Einschätzung in diesem Bereich. Mit unseren datengetriebenen und medizinisch fundierten Produkten stehen wir an der Spitze der Entwicklung von Automatisierung und effizientem Datenmanagement in der Versicherungsbranche. Für Versicherer liefern wir einen starken Mehrwert für alle Prozesse in der Personenschadenregulierung und tragen damit zum Wertschöpfungsprozess unserer Kunden bei.“[15]

Zur Bearbeitung von 610.000 Personenschadenfällen hat ACTINEO laut ihren Angaben auf der Website 924.000 Arztberichte angefordert, also im Durchschnitt etwa drei Arztberichte pro zwei Personenschadenfällen. Dabei wurden 60.000 Regressansprüche der Sozialversicherungsträger geprüft. Insgesamt ging es um eine Prüfsumme von 460 Millionen €, bei der „nachhaltige“ Kürzungen in Höhe von 47 Millionen € (also etwas mehr als 10 Prozent) erfolgt sein sollen.

4.1. Big Data – Big Brother

Neben Tätigkeiten, die zum Teil als Datenverarbeitung im Auftrag angesehen werden können, bietet ACTINENO auch das Produkt „ACTINEODATA“ an. Dieses bewirbt ACTINEO mit der folgenden Aussage:

„Wir entwickeln auf der Grundlage von Deutschlands größter unabhängiger Datenbank medizinisch codierter Personenschäden Prädiktionsmodelle und KI-Lösungen im Personenschaden.

Wir automatisieren Regulierungsprozesse und liefern digitale Instrumente für die Steuerung und das Controlling im Personenschaden.

Unser Geschäftsbereich ACTINEODATA umfasst

- *den Aufbau eines diagnosegestützten Datawarehouse*
- *die datenbasierte Unterstützung der Fallerkennung und Schadensteuerung*
- *Prozessschadenmanagement durch aktives Kostencontrolling*
- *Marktbenchmarks*
- *Datenanalysen und mathematisch-statistische Prognosemodelle für relevante Schadenkostenpositionen (Predictive Analytics)*
- *KI-Lösungen im Personenschaden“*[16]

Es ist stark zu vermuten, dass für diese Zwecke genau die Daten genutzt werden, die sie von den Haftpflichtversicherungen zur Erbringung anderer Dienstleistungen – wie z.B. ACTINEO-INFO – erhalten[17] oder im Auftrag der Haftpflichtversicherungen von den Sozialversicherungsträgern, aber auch von Krankenhäusern und Ärztinnen und Ärzten anfordern. Zur Frage des Datenschutzes in diesem Zusammenhang schreibt ACTINEO:

„Unser Unternehmen muss zur Erfüllung seiner vertraglichen Verpflichtungen gegenüber den beauftragenden Versicherungsunternehmen Gesundheitsdaten Ihrer Patienten erheben und verarbeiten. Dies erfolgt im Rahmen von Verträgen zur Auftragsverarbeitung gemäß den Vorgaben der Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) für die entsprechenden Versicherungsunternehmen.

Darüber hinaus werden wir von den Patienten/Geschädigten mit einer fallbezogenen Schweigepflichtentbindung legitimiert, die notwendigen Informationen von den behandelnden Ärzten und Kliniken zu erheben, zu erhalten und für die Dauer des Regulierungsprozesses zu speichern und zu verarbeiten.

Wir erheben grundsätzlich nur solche Daten, die zur Begründung von Schadenersatzansprüchen sowie zur Einschätzung des Sachverhaltes bei Personenschäden und der damit verbunden Leistungspflicht notwendig sind.“[18]

Hier würde besser passen: *„die zur Abwehr von Schadensersatzansprüchen (...) notwendig sind.“* Wenn, wie behauptet, die Datenverarbeitung nur im Rahmen von Auftragsverarbeitungen erfolgt und die Daten nur für die Dauer des Regulierungsprozesses gespeichert und verarbeitet werden, dann stellt sich doch die Frage, woher die Daten kommen, die für das Produkt „ACTINEODATA“ genutzt werden.

Auch unter dem Stichwort Datensicherheit sagt ACTINEO aus:

„Mit jedem Kunden wird ein Vertrag zur Auftragsverarbeitung geschlossen. Für Datensicherheit sorgt ein abgeschlossenes internes Netzwerk inklusive Firewall, Viren-, Server- und Systemüberwachung, hochmoderne Verschlüsselung von Daten, mehrmals tägliche vollautomatische Datensicherung auf getrennten Servern und nach Abschluss der Bearbeitung die Vernichtung der Daten/Belege gem. Art 4 DSGVO. Durch getrennte Datenhaltung ist sichergestellt, dass Kundendaten nur innerhalb des spezifischen Datenkreises verfügbar sind. So ist gewährleistet, dass die Daten der verschiedenen Kunden absolut zuverlässig getrennt voneinander verwaltet werden.“[19]

Das hört sich erst einmal gut an. Aber auch hier stellt sich die Frage, wie passt das mit der Aussage zusammen, dass ACTINEO ein diagnosegestütztes Datawarehouse aufbaut. Es müsste ja eigent-

lich für jeden Kunden ein eigenes Datawarehouse aufgebaut werden. Jedes Datawarehouse dürfte dann auch nur die Daten aus den aktuell zu bearbeitenden Fällen des jeweiligen Kunden enthalten. Und welche Daten sind in „Deutschlands größter unabhängiger Datenbank medizinisch codierter Personenschäden", wenn die Daten jeweils nach Abschluss der Bearbeitung des einzelnen Falles vernichtet werden?

4.2. Fehlende Transparenz

Transparenz sieht anders aus. Es ist für die betroffenen Personen, deren Daten im Datawarehouse, in „Deutschlands größter unabhängiger Datenbank medizinisch codierter Personenschäden" landen, zumindest anhand der öffentlich zugänglichen Informationen von ACTINEO nicht erkenntlich, was alles mit ihren Daten geschieht, die überwiegend nicht einmal von ihnen selbst, sondern von behandelnden Ärztinnen und Ärzten, vom Krankenhaus und/oder von ihrer Sozialversicherung an ACTINEO übermittelt werden.

Eine Anfrage im September 2019 an den Datenschutzbeauftragen der ACTINEO, die sich konkret auf die obigen Widersprüche bezog, wurde vom Datenschutzbeauftragten, der – wie sich aus der Antwort ergab – gleichzeitig Prokurist, Syndikusanwalt und „Leiter Recht und Datenschutz" der ACTINEO ist, lapidar mit folgender Aussage beantwortet:

„Wie Sie richtig schreiben, ist ACTINEO als Auftragsverarbeiter gem. Art. 28 DSGVO für verschiedene Haftpflichtversicherer tätig. Unsere Auftraggeber schätzen unsere hohen Standards beim Thema Datenschutz und unsere Diskretion.

Aus diesem Grund äußern wir uns gegenüber Dritten generell nicht zu Geschäftsinterna.

Gestatten Sie uns aber die allgemeine Bemerkung, dass ACTINEO in Sachen Datenschutz sehr gut aufgestellt ist. Unser Datenschutzmanagement wurde von den Datenschutzexperten unserer Kunden wiederholt überprüft sowie vom TÜV Rheinland zertifiziert: https://www.actineo.de/aktuelles/nachrichten/nachricht/news/tuev-geprueft-actineo-ist-dienstleister-mit-zertifiziertem-datenschutz-management/

Vor diesem Hintergrund dürfen wir Ihnen versichern, dass es sich bei dem von Ihnen skizzierten ‚Widerspruch' nur auf den ersten Blick um einen solchen handelt."

Nein, dieser Widerspruch ist nicht nur auf den ersten Blick ein Widerspruch. Auch auf den zweiten oder dritten Blick bleibt der Widerspruch, dass zum einen die personenbezogenen Daten pro Kunde (also pro Haftpflichtversicherung) strikt getrennt von den Daten der anderen Kunden verarbeitet werden, aber nur ein „diagnosegestütztes Datawarehouse" aufgebaut wird. Und dass zum anderen die Belege und Daten der geschädigten Personen nach Abschluss vernichtet werden, aber „Deutschlands größte unabhängige Datenbank medizinisch codierter Personenschäden" genutzt wird. Indirekt bestätigt aus Sicht des Autors die Aussage des Datenschutzbeauftragten von ACTINEO die Vermutung, dass die Daten, die in ACTINEOs Datenbank medizinisch codierter Personenschäden landen, aus der Tätigkeit für die Haftpflichtversicherungen stammen. Denn sonst müsste sich der Datenschutzbeauftragte nicht auf die Diskretion gegenüber den Auftraggebern von ACTINEO berufen.

4.3 Zertifizierung

Die ACTINEO hat von der TÜV Rheinland i-sec GmbH ein Datenschutzzertifikat als „Dienstleister mit geprüftem Datenschutzmanagement" erhalten. Allerdings stellt dieses Zertifikat – wie die TÜV Rheinland i-sec GmbH selbst schreibt – *„kein akkreditiertes Zertifizierungsverfahren, Siegel oder Prüfzeichen im Sinne der Art. 42, 43 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) dar"*.[20] Auch sind die Kriterien, nach denen die Prüfungen vorgenommen wurden, nicht öffentlich zugänglich. Als ergänzende Information ist bei einem Klick auf „Dienstleister mit geprüftem Datenschutzmanagement" nur zu finden:

„Dienstleister, die dieses Prüfzeichen führen dürfen, bieten höchste Sicherheit bei der Erhebung, Speicherung, Verarbeitung und Weitergabe von personenbezogenen Daten. Der betriebliche Datenschutz entspricht den organisatorischen und technischen Anforderungen gemäß Bundesdatenschutz- und Telekommunikationsgesetz. Geprüft wird nach den Richtlinien des Standards ISO IEC 27001:2005 und unseres Anforderungskatalogs für das Zertifikat Dienstleister mit geprüftem Datenschutzmanagement."[21]

Es wird also – zumindest nach der eigenen Aussage der TÜV Rheinland i-sec GmbH – keineswegs geprüft, ob die Verarbeitung personenbezogener Daten den rechtlichen Anforderungen des Datenschutzes genügt. Von daher sagt diese Zertifizierung zur datenschutzrechtlichen Zulässigkeit der Verarbeitungsprozesse der ACTINEO leider gar nichts aus. Einzig und allein die technischen und organisatorischen Maßnahmen werden als dem Datenschutz entsprechend bestätigt. In diesem Zusammenhang sei nur am Rande erwähnt, dass zumindest die Datenschutzaufsichtsbehörden und viele Datenschutzexperten es als kritisch ansehen, wenn der oder die Datenschutzbeauftragte der Leitung eines Unternehmens angehört, was bei einem Prokuristen offensichtlich gegeben ist. Also ist bei der ACTINEO auch beim Datenschutzmanagement noch Luft nach oben.

Dass die DSGVO in dieser Information nicht erwähnt wird, ist vermutlich nur ein Versehen. Auch dass ein Klick auf *„Weitere Informationen zur Zertifizierung ‚Dienstleister mit geprüftem Datenschutzmanagement' finden Sie hier."* weiter unten auf der Seite nur auf eine Fehlerseite[22] führt, ist sicher ebenfalls nur ein Versehen.

Festzuhalten bleibt:

Ohne Offenlegung der Kriterien, nach denen eine solche Zertifizierung erfolgt, ist diese Zertifizierung weder für betroffene Personen noch für Auftraggeber hilfreich.

Eine Prüfung der rechtlichen Zulässigkeit erfolgt nicht.

Es ist zwar davon auszugehen, dass Kunden, die Wert auf Datenschutz legen, die Prüfberichte anfordern und vermutlich auch vorgelegt bekommen. Es ist allerdings nicht davon auszugehen, dass betroffene Personen diese Prüfberichte erhalten.

5. Der Einzelne oder die betroffene Person

Im Volkszählungsurteil spricht das Bundesverfassungsgericht von dem

Einzelnen. Die DSGVO spricht von der betroffenen Person: So sind

„‚personenbezogene Daten' alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen".[23]

Wer sich jetzt die Frage stellt, was denn eine „identifizierbare natürliche Person" sei, findet die Antwort direkt im Anschluss:

„als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt [identifiziert werden kann], insbesondere mittels Zuordnung

- *zu einer Kennung wie einem Namen,*
- *zu einer Kennnummer,*
- *zu Standortdaten,*
- *zu einer Online-Kennung oder*
- *zu einem oder mehreren besonderen Merkmalen (…), die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;"*[24]

Egal ob „Einzelner" oder „betroffene Person", es geht beim Thema Datenschutz immer um den Menschen und um den Schutz seiner Grundrechte.

In einem Personenschadensfall gibt es viele betroffene Personen: Wir haben mindestens eine geschädigte Person und meist auch eine unfallverursachende Person. Bei einem Personenschaden wird es dann auch Personen geben, die die geschädigte Person behandelt oder transportiert haben. Weiterhin gibt es Personen, die die entsprechenden Leistungen abrechnen. Bei einer umfassenden datenschutzrechtlichen Erörterung der Datenverarbeitung von Gesundheitsdaten durch die Haftpflichtversicherungen und durch ihre Dienstleister müssten alle diese betroffenen Personen berücksichtigt werden. Hier soll es aber in erster Linie um die geschädigte betroffene Person gehen.

5.1. Datenverarbeitung im Einzelfall

Es ist sicher unstreitig, dass bestimmte, unfallbezogene Daten der betroffenen Person sowohl für die Behandlung als auch für deren Abrechnung von den Leistungserbringern (u.a. Arztpraxen, Krankenhäuser, Krankentransporte) erfasst und verarbeitet werden müssen. Dass ein Teil dieser Daten dann auch von den Sozialleistungsträgern (insbesondere gesetzliche Krankenversicherungen, gesetzliche Unfallversicherungen) verarbeitet werden müssen, dürfte auch nicht in Frage gestellt werden. Die entsprechenden Erlaubnistatbestände für die Verarbeitung sollten sich aus Art. 6 Abs. 1 DSGVO und für die Gesundheitsdaten aus Art 9 Abs. 2 DSGVO jeweils in Verbindung mit den Fachgesetzen, insbesondere den entsprechenden Sozialgesetzbüchern, ergeben. Auch dass bei einem Unfallgeschehen im erforderlichen Umfang personenbezogene Daten der geschädigten Peron an die Haftpflichtversicherung der unfallverursachenden Person weitergegeben werden müssen, damit der Sozialleistungsträger diese Haftpflichtversicherung in Regress nehmen kann, ist unvermeidlich, gesetzlich durch § 116 SGB X geregelt und solange nicht zu beanstanden, solange hierbei nur die zwingend erforderlichen Daten von den Haftpflichtversicherungen und ihren Dienstleistern angefordert und verarbeitet werden.

Kornes legt in seinem Beitrag für die Fachtagung Personenschaden am 07./08.11.2019[25] allerdings umfassend dar, dass seitens des Dienstleisters oft Daten und Belege angefordert werden, die – aus Sicht der Sozialleistungsträger – für die Beurteilung der Erstattungspflicht nicht relevant seien. In diesem Fall wäre bereits deren Anforderung, spätestens aber deren Verarbeitung durch die Haftpflichtversicherungen und/oder ihren Dienstleister ein Verstoß gegen den Grundsatz der Datenminimierung aus Art. 5 Abs. 1 Buchst. c) DSGVO.

Auch das Landgericht Bremen hat in einer Entscheidung vom 10.07.2019 (Aktenzeichen 1 O 2112/16) befunden:

„Bei Regressen nach § 116 SGB X kann die klagende Krankenkasse die Schadenshöhe durch Vorlage einer Auflistung der Schadenspositionen unter Beilage der ihr nach den §§ 285 Abs. 1 Nr. 11, 295, 300 ff SGB V elektronisch übersandten Abrechnungsdaten der jeweiligen Leistungserbringer nachweisen."[26]

Laut Prelinger ergibt sich aus diesem Urteil in Verbindung mit früheren Urteilen des Bundessozialgerichts (BSG), u.a. dass § 301 SGB V eine abschließende Liste enthält, welche Daten Krankenhäuser zur Abrechnung an gesetzliche Krankenversicherungen übermitteln dürfen. Die Anforderung weiterer Unterlagen durch die Krankenversicherungen sei daher unzulässig. Im Falle einer rechtlich zulässigen Überprüfung einer Abrechnung sind weitere Unterlagen nur an den Medizinischen Dienst der Krankenversicherungen (MDK), aber nicht an die Krankenversicherung zu übermitteln. Der MDK wiederum darf nur das Ergebnis seiner Überprüfung, nicht aber die Sozialdaten im Einzelnen an die Krankenversicherung übermitteln. Prelinger stellt fest, dass das „verfassungsbedingt strenge sozialrechtliche System der Datenverwendung und die abschließende Rechnungsprüfung durch den MDK (...) bei der zivilrechtlichen Geltendmachung nach § 116 SGB X übergegangener Ansprüche fort[wirkt]."[27] Oder mit anderen Worten: Auch die in Regress genommenen Haftpflichtversicherungen müssen sich bei Krankenhausabrechnungen mit den in § 301 SGB X genannten Daten begnügen. Die Anforderung weiterer Unterlagen zur Bearbeitung der Regressfälle durch den Dienstleister der Haftpflichtversicherungen sowie die entsprechende Weitergabe dieser Unterlagen durch Krankenhäuser oder gesetzliche Krankenversicherungen sind demnach rechtlich nicht zulässig

5.2. Datawarehouse und „KI"

ACTINEO wirbt – wie bereits dargestellt – damit, dass sie „Deutschlands größte unabhängige Datenbank medizinisch codierter Personenschäden" haben und auf dieser Basis nicht nur „Marktbenchmarks" entwickeln, sondern auch Datenanalysen erstellen und „mathematisch-statistische Prognosemodelle für relevante Schadenkostenpositionen (Predictive Analytics)" anbieten. Darüber hinaus gehören „KI-Lösungen im Personenschaden" zum Angebot.[28]

Es geht also nicht mehr um die Bearbeitung eines Einzelfalles, um die Verarbeitung der Daten einer betroffenen geschädigten Person zum konkreten Zweck der Unterstützung der Haftpflichtversicherung im Regressprozess mit dem Sozialleistungsträger. Mit Hilfe der sogenannten künstlichen Intelligenz sollen die Daten des Data-

warehouse zum Nutzen der Haftpflichtversicherer ausgewertet, die Daten für „Marktbenchmarks" verwendet und Vorhersagemodelle entwickelt werden.

Hier stellt sich direkt die Frage nach der Zweckbindung der Daten, die für die Regulierung des einzelnen Schadenfalles entweder von den Sozialversicherungsträgern, den Leistungserbringern oder gar der geschädigten Person an die Haftpflichtversicherung oder ihren Dienstleister herausgegeben wurden. Für Gesundheitsdaten, die zu den besonderen Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO gehören, gelten besonders strikte Regelungen, auch in Bezug auf mögliche Zweckänderungen. Eine Erlaubnis auf Grund einer Interessenabwägung, wie sie nach Art. 6 Abs. 1 Buchst. f) DSGVO bei „normalen" personenbezogenen Daten möglich wäre, ist bei Gesundheitsdaten wegen Art. 9 Abs. 1 DSGVO nicht möglich. Art. 9 Abs. 1 DSGVO sagt eindeutig: *„(…), die Verarbeitung von (…) Gesundheitsdaten (..) ist untersagt"*. Zwar enthält Art. 9 Abs. 2 DSGVO insgesamt 10 Ausnahmen von dieser Untersagung[29], aber keine der dort genannten Ausnahmen ist auf „Deutschlands größte unabhängige Datenbank medizinisch codierter Personenschäden" anwendbar. Hieraus folgt, dass eine Zweckänderung zur Verarbeitung der personenbezogenen Daten in der genannten Datenbank nur mit ausdrücklicher, informierter Einwilligung der betroffenen Personen nach Art. 9 Abs. 2 Buchst. b) in Verbindung mit Art. 7 DSGVO zulässig wäre.

Es bleibt also nur die Anonymisierung der Daten. Hierzu ist vorab festzustellen, dass eine wirksame und irreversible Anonymisierung von sehr spezifischen personenbezogenen Daten – und um solche handelt es sich bei den Personenschadensfällen offensichtlich – nur schwer möglich ist. Denn der Begriff der identifizierbaren natürlichen Person und damit der Begriff des personenbezogenen Datums ist – wie weiter oben dargestellt – sehr weit gefasst. Welche Zusatzinformationen reichen der Haftpflichtversicherung oder dem Dienstleister, der die Datenbank betreibt, aus, um zu einer konkreten Person den angeblich anonymisierten Datensatz aus dieser Datenbank wieder zuzuordnen?

Die DSGVO sagt hierzu:

„Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern.

Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind." [30]

Aber selbst, wenn davon ausgegangen werden könnte, dass eine wirksame und irreversible Anonymisierung dieser Daten möglich ist und nur derartig anonymisierte Datensätze sich in der Datenbank befinden, heißt das dann automatisch, dass die Anonymisierung selbst datenschutzrechtlich zulässig ist? Offensichtlich ist, dass die DSGVO nur für personenbezogene, nicht aber für anonyme Daten gilt:

„Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke."[31]

Soweit so gut. Allerdings stellt der Vorgang des Anonymisierens selbst eine Datenverarbeitung im Sinne des Art. 4 Ziff. 2 DSGVO dar und bedarf daher auch einer entsprechenden Rechtsgrundlage.

Die Anonymisierung zum Zwecke der Einspeicherung der anonymisierten Daten in eine Datenbank stellt somit eine Verarbeitung von personenbezogenen Daten dar, die unweigerlich zu einer Änderung des ursprünglichen Zweckes der Datenverarbeitung – nämlich Bearbeitung des konkreten Schadenfalles – führt. Für diese Zweckänderung bedarf es einer Rechtsgrundlage. Und als solche kommt – wie oben dargestellt – nur die informierte und ausdrückliche Einwilligung der betroffenen Personen in Frage.

5.3. Legal? Legitim?

Selbst wenn wir an dieser Stelle annehmen würden, dass die Aufnahme anonymisierter Daten aus den konkreten einzelnen Schadensfällen in „Deutschlands größte unabhängige Datenbank medizinisch codierter Personenschäden" datenschutzrechtlich formal nicht zu beanstanden wäre, stellt sich immer noch die Frage:

Ist es legitim, dass sensible Daten, die nur deswegen an die Haftpflichtversicherung der einen Personenschaden verursachenden Person oder an den Dienstleister dieser Haftpflichtversicherung gegeben werden, um den konkreten Einzelfall zu regulieren, in einem Datawarehouse landen und unter Anwendung von „KI" verwendet werden, um zum Nutzen der Haftpflichtversicherungen die Regressansprüche der Sozialversicherungsträger soweit wie möglich zu reduzieren und um Marktbenchmarks zu erstellen?

Hier wird das konkrete menschliche Schicksal im Einzelfall auf einen „medizinisch codierten Personenschaden" unter vielen reduziert. Das Subjekt – die geschädigte betroffene Person – wird zum Objekt von „Prädiktionsmodellen und KI-Lösungen". Anstelle der individuellen von einer fachkundigen Person erfolgenden Einzelfallentscheidung in der Haftpflichtversicherung kommen automatisierte Einzelfallentscheidungen – die sogenannte Dunkelverarbeitung[32] – zum Einsatz. Sofern der Sozialleistungsträger und nicht die betroffene geschädigte Person, deren Daten gerade „dunkel" verarbeitet werden, der Adressat der Entscheidung über die Höhe der Regresszahlung ist, läuft das Recht der betroffenen Person, „nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden" aus Art. 22 Abs. 1 DSGVO ins Leere. Denn die Entscheidung der „Dunkelverarbeitung" entfaltet ihre rechtliche Wirkung bei den Regressverfahren

eines Sozialleistungsträgers gegen die jeweilige Haftpflichtversicherung in der Regel nicht gegenüber der betroffenen Person, sondern gegenüber diesem Sozialleistungsträger, der mit der Bezahlung der Behandlung der Unfallschäden bereits in Vorleistung gegangen ist.

6. Fazit

Anhand der vorliegenden Informationen ist zu vermuten, dass ein solches System, dass „Deutschlands größte unabhängige Datenbank medizinisch codierter Personenschäden" zur Erstellung von „Prädiktionsmodellen" und zur Nutzung für Entscheidungsfindungen unter Anwendung von „KI" datenschutzrechtlich unzulässig ist, da nicht davon ausgegangen werden kann, dass die betroffenen Personen ihre informierte Einwilligung in die Zweckänderung der für die Bearbeitung der Regressansprüche angeforderten Daten erteilt haben. Hier sollte aus Sicht des Autors die zuständige Datenschutz-Aufsichtsbehörde aktiv werden und dieses System einer datenschutzrechtlichen Prüfung unterziehen.

Legitim ist – wenn zur Beurteilung dieser Fragestellung der Einzelne, die betroffene Person in den Mittelpunkt gestellt wird – ein solches System unter dem Gesichtspunkt des Rechts auf informationelle Selbstbestimmung aus Sicht des Autors nicht mehr.

1 Dieser Artikel ist eine überarbeitete Fassung von Teil 2 der Erstveröffentlichung in: Huber, Kornes, Mathis, Thoenneßen (Hrsg.): Fachtagung Personenschaden, Nomos Verlagsgesellschaft, Seiten 106 - 122

2 Kornes schrieb zwar, dass ACTINEO der einzige Dienstleister diese Art sei. Auf der Fachtagung Personenschaden am 07./08.11.2019 ergab sich aber, dass es noch mindestens einen weiteren Dienstleister gibt (vgl. Kornes, Belegforderungswelle und massive Datenerhebungen bei Regress-Forderungen: Ein Report aus SVT-Sicht in: Huber, Kornes, Mathis, Thoenneßen (Hrsg.): Fachtagung Personenschaden, Nomos Verlagsgesellschaft)

3 https://www.actineo.de/, abgerufen am 09.02.2020

4 https://www.actineo.de/, abgerufen am 09.02.2020

5 Werner Hülsmann: Datenschutzrechtliche Aspekte der Verarbeitung von Gesundheits- und Sozialdaten bei Personenschäden durch Sozialversicherungen und in Regress genommene Haftpflichtversicherungen, in Datenschutznachrichten, Ausgabe 1/2020

6 So zum Beispiel: https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2019/20190508-gesundheitswirtschaft-wachstumsfaktor-und-jobmotor-in-deutschland.html (abgerufen am 21.09.2019)

7 https://www.bmwi.de/Redaktion/DE/Textsammlungen/Branchenfokus/Wirtschaft/branchenfokus-gesundheitswirtschaft.html (abgerufen am 09.02.2020)

8 https://www.jura.uni-hamburg.de/forschung/institute-forschungsstellen-und-zentren/sozialrecht-sozialpolitik/pdf-dokumente/obstvortrag.pdf (erstellt vermutlich 2015, abgerufen am 21.09.2019). Eine Quelle für diese Aussage wird in der Präsentation nicht angegeben. Bei der Suche nach einer Quelle zu dieser Aussage ist der Autor auf eine Studie von Kruse, Knappe, Schulz-Nieswandt, Schwartz und Wilbers aus dem Jahr 2003 (https://www.uni-trier.de/fileadmin/fb4/prof/VWL/SAM/veroeffentl/Kruse-Knappe-Schulz-Nieswandt-Schwartz-Wilbers-Kostenentw-Ge.pdf, Seite 28, abgerufen am 09.02.2020) gestoßen, die sich wiederum auf eine Studie von Lauterbach et. al aus dem Jahr 2001 beruft.

9 Online verfügbar unter https://openjur.de/u/268440.html

10 BVerfGE 65, 1; zitiert nach https://openjur.de/u/268440.html, Randnummer 1

11 BVerfGE 65, 1; zitiert nach https://openjur.de/u/268440.html, Randnummer 94, Sätze 1-3

12 BVerfGE 65, 1; zitiert nach https://openjur.de/u/268440.html, Randnummer 95 Satz 2

13 BVerfGE 65, 1; zitiert nach https://openjur.de/u/268440.html, Randnummer 107, Satz 2

14 https://www.actineo.de/unternehmen/ueber-uns/, abgerufen am 09.02.2020

15 https://www.actineo.de/unternehmen/ueber-uns/, abgerufen am 09.02.2020

16 https://www.actineo.de/produkte/actineodata/, abgerufen am 21.09.2019

17 vgl. https://www.actineo.de/produkte/actineoinfo/, abgerufen am 21.09.2019

18 https://www.actineo.de/arztinfo/informationen-fuer-aerzte-und-kliniken/, abgerufen am 21.09.2019

19 https://www.actineo.de/qualitaet/datensicherheit/, abgerufen am 21.09.2019

20 https://www.certipedia.com/quality_marks/0000054127?locale=de, abgerufen am 09.02.2020

21 https://www.certipedia.com/keywords/944?locale=de, abgerufen am 09.02.2020

22 https://www.certipedia.com/admin_area/quality_marks/284516/ https:/www.tuv.com/germany/de/datenschutz-zertifizierung-f%C3%BCr-unternehmen.html, erstmals abgerufen am 21.09.2019, erneut abgerufen am 09.02.2020

23 vgl. Art. 4 Ziff. 1 DSGVO,

24 Art. 4 Ziff. 1, 2. Halbsatz DSGVO, Aufzählungszeichen durch den Autor eingefügt, Satzstellung zum besseren Verständnis entsprechend der englischen Fassung angepasst.

25 vgl. Kornes a.a.O.

26 Prelinger, Wolfdietrich: „Beweisführung durch Ausdrucke elektronisch übermittelter Abrechnungsdaten im Regress nach § 116 SGB X" in Möller und Partner - Kanzlei für Medizinrecht (Hrsg.): juris PraxisReport Medizinrecht, 12/2019 Anm. 3

27 Prelinger, a.a.O.

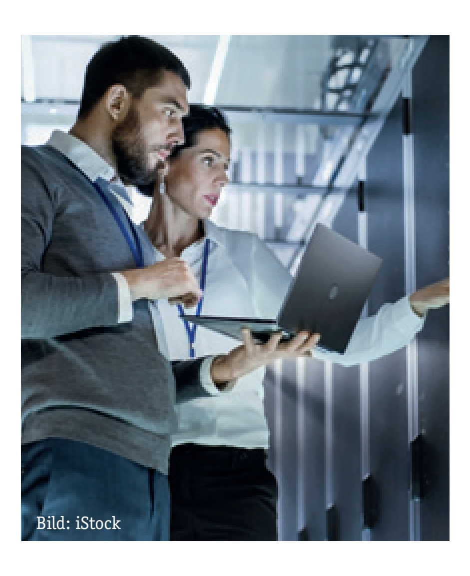
28 vgl. https://www.actineo.de/produkte/actineodata/, abgerufen am 22.09.2019

29 Vgl. Hülsmann, a.a.O.

30 Erwägungsgrund 26 Sätze 3,4 DSGVO

31 Erwägungsgrund 26 Sätze 5, 6 DSGVO

32 In der Versicherungswirtschaft die Bezeichnung für einen Geschäftsprozess in der Vorgangsbearbeitung, der vollständig automatisiert abläuft. Der Prozess bleibt im Dunkeln, weil der Ablauf von den Anwenderinnen und Anwendern weder beeinflusst noch die Durchführung verfolgt werden kann.


Bild: iStock

Thilo Weichert

„Digitale-Versorgung-Gesetz“ und Datentransparenz

1 Was bisher geschah

Am 19.12.2019 trat das „Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation“, abgekürzt „Digitale-Versorgung-Gesetz“ (DVG) in Kraft.[1] Die grammatikalisch falsche Kurzbezeichnung des Gesetzes liegt auf der aktuellen Linie der Bundesregierung, ihre Gesetze mit „Neusprech“ zu labeln. Mit dem Gesetz erfolgen Änderungen des Sozialgesetzbuches (SGB) V zur „Gesetzlichen Krankenversicherung“ (GKV). Nicht erfasst ist also der gesamte Bereich der privaten Gesundheitsversorgung. Dem verantwortlich zeichnenden Bundesgesundheitsministerium (BMG) und seinem Minister Jens Spahn geht es darum, die medizinische Versorgung „digitaler und besser“ zu machen.[2] Das in der **Digitalisierung hinterherhinkende Deutschland** solle doch zumindest im Gesundheitsbereich im globalen Wettbewerb aufholen. Dafür ist ein Strauß unterschiedlicher Maßnahmen Gesetz geworden, etwa dass Ärzte künftig Apps für Menschen mit Bluthochdruck oder Diabetes verschreiben können und die Kosten von der Krankenkasse zu übernehmen sind oder dass Videosprechstunden in Anspruch genommen werden können. Letztlich stimmten Linke und Grüne gegen das Gesetz. AfD und FDP enthielten sich.[3]

Ein zentraler Bestandteil des Gesetzes ist eine völlige Neufassung der §§ 303a-303f SGB V mit der Überschrift **„Datentransparenz“**. Dieser zweite Titel des 10. Kapitels des SGB V wurde 2003 eingeführt.[4] Das 10. Kapitel des SGB V steht unter der Überschrift „Versicherungs- und Leistungsdaten, Datenschutz, Datentransparenz“. Das Thema „Datentransparenz“ war erstmals grundlegend behandelt worden durch die grüne Gesundheitsministerin Andrea Fischer und wurde letztlich ohne großes öffentliches Aufsehen unter der SPD-Gesundheitsministerin Ulla Schmidt von der rot-grünen Regierungsmehrheit im Bundestag beschlossen. Der Vorschlag, eine pseudonyme Datenverarbeitung für übergreifende Auswertungen zu etablieren, ging letztlich auf Vorschläge von Datenschützern zurück, u.a. auch der Deutschen Vereinigung für Datenschutz (DVD), die entsprechende Vorschläge am 22.09.1999 erstmals im Bundestag präsentierten.[5] Das Potenzial der dadurch gespeicherten pseudonymen Krankenkassendaten wurde daraufhin über Jahre hinweg nicht ausgeschöpft, was einerseits an dem begrenzten Datensatz und an den damit verbundenen begrenzten Auswertungsmöglichkeiten, aber auch an der geringen Bekanntheit des Instruments lag. Dies ändert sich nun schlagartig durch das Digitale-Versorgung-Gesetz (DVG), mit dem die Öffentlichkeit und die Welt der Forschenden die Datentransparenz plötzlich entdecken.

Die Reaktion auf diese gesetzliche Aufwertung ist heftig. Das **Gespenst der zentralen Datenspeicherung** aller Krankenversichertendaten einschließlich der elektronischen Patientenakten, mit dem über Jahre hinweg der elektronischen Gesundheitskarte (eGK) und der Telematik-Infrastruktur (TI) das Leben und Entwickeln schwer gemacht wurden, stand plötzlich im Fokus der öffentlichen Wahrnehmung.[6] Tatsächlich schienen die Vorschläge des BMG nicht gerade ausgewogen. So fragte die Süddeutsche Zeitung, ob es sein kann, dass „die persönlichen Gesundheitsdaten von mehr als 70 Millionen Bürgern zentral gespeichert werden“. Sollte da tatsächlich eine der größten Datensammlungen der Bundesrepublik entstehen, und das auch noch mit den höchstpersönlichen Krankendaten der Bevölkerung und weitgehend ungeschützt?[7]

Erst kurz vor der endgültigen Beschlussfassung im Bundestag wurde dies zum öffentlich kontrovers diskutierten Thema. Drei Tage vor der entscheidenden Sitzung entschärfte die Bundesregierung den Gesetzesvorschlag. Die Angaben zu Alter, Geschlecht, Leistungsbezug, Behandlungen und Gesundheitsstatus sollen nicht mehr mit dem eindeutig zuordenbaren **Versichertenkennzeichen** übermittelt werden können, sondern nur noch unter Pseudonym.

Dass dies in letzter Minute korrigiert werden musste, lag an der Art des **Vorgehens des BMG** und seines Ministers. Die Berücksichtigung der Expertise des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) Ulrich Kelber wurde ebenso übergangen wie überhaupt die Kommunikation mit den Beteiligten und Betroffenen. So kritisierte in Bezug auf diese Gesetzgebung der Vorsitzende des Deutschen Ethikrats Peter Dabrock, Spahn handle über die Köpfe der Bürger hinweg.[8] Schon zuvor hatte das BMG seine auch zunächst im DVG verfolgten Pläne zur Einführung einer elektronischen Patientenakte (ePA) nach heftigem Widerstand des Verbraucher- und Justizministerium aufgeben müssen, weil zu großer „Änderungs- und Ergänzungsbedarf“ bestand, etwa weil „gesetzliche Vorgaben für ein Einwilligungs- und Berechtigungsmanagement zur Wahrung der Datenhoheit des Versicherten“ schlicht nicht vorgesehen waren.[9]

2 Der rechtliche Rahmen

Tatsächlich ist schon seit 2003 geregelt, dass Patientendaten aus dem Bereich der GKV in pseudonymer Form zentral gespeichert sind und ausgewertet werden können. Die Gesetzesänderung sieht nun eine **Ausweitung sowohl des Datensatzes als auch der möglichen Nutzungen** vor. Da eine Auswertung von Gesundheitsdaten von hoher gesellschaftlicher Wichtigkeit sein kann, ist hiergegen zunächst grundsätzlich nichts einzuwenden.

Der europäische Gesetzgeber hat festgelegt, dass die Auswertung solcher Daten ausschließlich „aus **Gründen des öffentlichen Interesses**“ zulässig ist. Im Bereich der öffentlichen Gesundheit ergibt sich dies direkt aus Art. 9

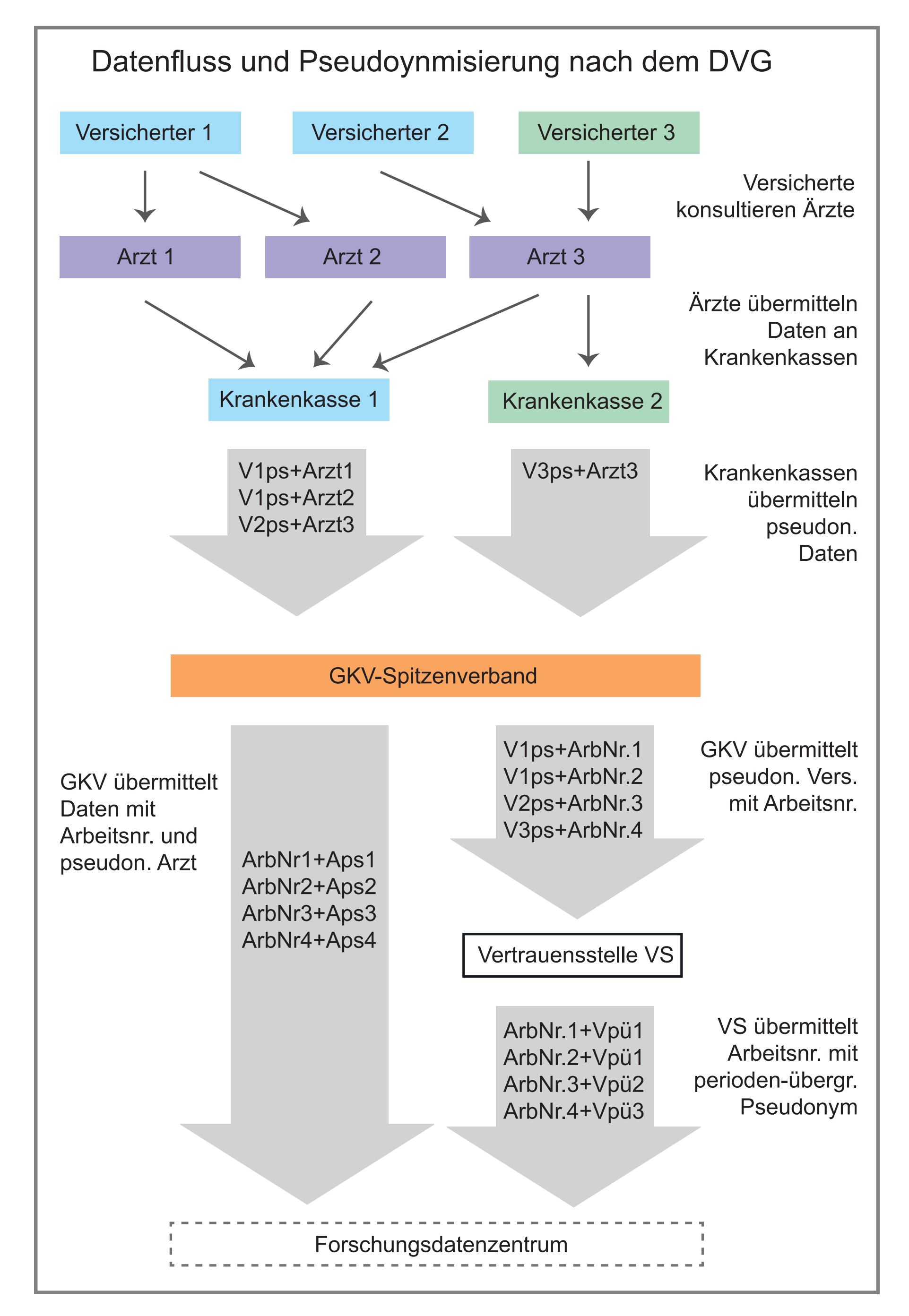
Abs. 2 lit. i DSGVO, was dort weiter beispielhaft präzisiert wird. Es geht z.B. um den „Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren", um die „Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten". Auch bei einer Verwendung für wissenschaftliche Forschungszwecke nach Art. 9 Abs. 2 lit. j DSGVO muss, wenn eine privilegierte Datennutzung erfolgen soll, die Art. 5 Abs. 1 lit. b DSGVO für Forschungszwecke ausdrücklich vorsieht, ein überwiegendes öffentliches Interesse vorliegen.[10]

Voraussetzung ist, dass dabei, wie in Art. 9 Abs. 2 lit. i, j DSGVO gefordert wird, „**angemessene und spezifische Maßnahmen** zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses" festgelegt und umgesetzt werden. Insofern sind einige Vorkehrungen im DVG geregelt, doch sind diese verbesserungsfähig und -bedürftig.

Die Aufgaben der Datentransparenz werden von einer **Vertrauensstelle** und einem **Forschungsdatenzentrum** (früher: Datenaufbereitungsstelle) wahrgenommen. Bei beiden handelt es sich um öffentliche Stellen des Bundes. Die Benennung erfolgt per Rechtsverordnung durch das BMG. Sie sind räumlich, organisatorisch und personell eigenständig, d.h. auch voneinander getrennt zu führen und unterliegen ausschließlich der Rechtsaufsicht des BMG (§ 303a Abs. 1, 2). Das Fehlen einer Fachaufsicht bedeutet, dass die beiden Stellen keine fachlichen Weisungen des BMG oder irgendeiner anderen Stelle entgegennehmen. Diese rechtliche Unabhängigkeit hätte man zweifellos klarer und besser ins Gesetz schreiben können.

Die Krankenkassen liefern über den Spitzenverband Bund der Krankenkassen (**GKV-Spitzenverband**) zu jedem Versicherten die Daten an. Dabei verwenden sie ein Versichertenpseudonym, „das eine kassenübergreifende eindeutige Identifizierung" erlaubt (Lieferpseudonym). Der GKV-Spitzenverband prüft die Daten auf Vollständigkeit, Plausibilität und Konsistenz und klärt offene Fragen mit der jeweiligen liefernden Krankenkasse. Der GKV-Spitzenverband übermittelt dann ohne Lieferpseudonym mit einer Arbeitsnummer den Datensatz mit Angaben zu Alter, Geschlecht und Wohnort des Patienten, Angaben zum Versicherungsverhältnis sowie den Kosten- und Leistungsdaten nach den §§ 295, 295a, 300, 301, 301a und 302 SGB V an das Forschungsdatenzentrum. Auch die Angaben zu den Leistungserbringern (also Ärzten, Apotheken usw.) werden vor der Übermittlung pseudonymisiert. Der GKV-Spitzenverband liefert zudem eine Liste der Lieferpseudonyme mit deren Zuordnung zu den Arbeitsnummern an die Vertrauensstelle (§ 303b).

Gegenüber dem bisher eingemeldeten Datensatz soll es eine massive Ausweitung geben: Bisher stand für dessen Umfang und Inhalt der Risikostrukturausgleich (§ 268 SGB V) im Vordergrund. Jetzt können grds. **alle Kosten- und Leistungsdaten** übermittlungspflichtig gemacht werden. Voraussetzung ist lediglich, dass in einer Rechtsverordnung Art und Umfang der Daten (Datenfelder und Detailtiefe) bestimmt werden (§ 303a Abs. 4 Nr. 1 SGB V). Erfasst werden damit die Krankenhausbehandlung (§ 301), die ambulante Versorgung (§§ 295, 295a), die Versorgung mit Arz-



neimitteln (§ 300), Heil- und Hilfsmittel incl. Digitalanwendungen (§ 302), die Versorgung durch Hebammen (§ 301a) sowie andere Leistungserbringer (etwa Physiotherapeuten, § 302). Die Ausweitung umfasst nun auch Angaben zu den Leistungserbringern.[11] Bzgl. der Angaben zum Wohnort der Patientinnen und Patienten sollen insbesondere in Großstadtgemeinden und Flächenkreisen Zuordnungen zu Lebens- und Sozialräumen möglich sein. Die Angaben zum Versichertenverhältnis können Angaben zum Versichertenstatus, Vitalstatus einschließlich des Sterbedatums der Versicherten umfassen.[12] Der bisherige Datenkranz wird mittels Rechtsverordnung durch ein „deutlich erweitertes und aktuelleres Datenangebot" ersetzt.[13]

Die **Vertrauensstelle** überführt die Lieferpseudonyme nach einem einheitlich anzuwendenden Verfahren in **periodenübergreifende Pseudonyme**. Das dabei verwendete Verschlüsselungsverfahren „ist so zu gestalten, dass für das jeweilige Lieferpseudonym eines jeden Versicherten periodenübergreifend immer das gleiche Pseudonym erstellt wird, aus dem Pseudonym aber nicht auf das Lieferpseudonym oder die Identität des Versicherten geschlossen werden kann" (§ 303c Abs. 2). Die Vertrauensstelle übermittelt dann die Pseudonyme mit den Arbeitsnummern dem Forschungsdatenzentrum und löscht danach die Lieferpseudonyme, Arbeitsnummern und übermittelten Pseudonyme (§ 303c Abs. 3 SGB). So soll verhindert werden, dass über das periodenübergreifende Pseudonym auf die Person des Versicherten rückgeschlossen werden kann. Wie die Pseudonyme mit welchen Algorithmen generiert werden, ist im Gesetz nicht festgelegt und wird der Rechtsverordnung überlassen (§ 303a Abs. 4 Nr. 3).

Das **Forschungsdatenzentrum** hat nach § 303d Abs. 1 SGB V die Aufgabe, die angelieferten Daten zu speichern, aufzubereiten und auszuwerten. Zu den Aufgaben gehören u.a.

- die Qualitätssicherung der Daten (Nr. 2)
- die Prüfung von Anträgen auf Datennutzung (Nr. 3),
- das Führen eines Antragsregisters mit Informationen zu den Nutzungsberechtigten incl. Vorhaben und deren Ergebnisse (Nr. 6) und
- die Bereitstellung der benötigten Daten an die Nutzungsberechtigten (§ 303e Abs. 1 SGB V).

Im Rahmen der Aufbereitung der Daten erstellt das Zentrum anonymisierte Datensätze, sog. Public Use Files, die es öffentlich verfügbar macht, etwa für Schulungs-, Entwicklungs- und Testzwecke.[14] Zudem hat es Aufgaben der Evaluation, der Weiterentwicklung der Datentransparenz, der Beratung und der Schulung der Nutzungsberechtigten. Im Rahmen der Antragsprüfung hat das Forschungsdatenzentrum das **Reidentifizierungsrisiko** bei jeder Datenpreisgabe zu „bewerten und unter angemessener Wahrung des angestrebten wissenschaftlichen Nutzens durch geeignete Maßnahmen zu minimieren" (§ 303d Abs. 1 Nr. 5).

Die **Speicherdauer** ist maximal 30 Jahre (§ 303d Abs. 4). Der Gesetzgeber geht davon aus, dass nach spätestens 30 Jahren auch für wissenschaftliche Forschungszwecke eine Erforderlichkeit nicht mehr gegeben ist. Innerhalb des Rahmens kann eine Präzisierung durch die Rechtsverordnung erfolgen. Schon jetzt bestehen Forderungen, längere Aufbewahrungsfristen zu ermöglichen.[15] Für die Aufgabenerledigung kann das Zentrum Auftragsverarbeiter (§ 80 SGB X) einschalten.[16]

Die Liste der potenziell **Nutzungsberechtigten** (§ 303e Abs. 1) ist umfangreich:

- GKV-Spitzenverband
- Bundes- und Landesverbände der Krankenkassen
- Kassenärztliche Bundesvereinigung und Kassenärztliche Vereinigungen,
- Spitzenorganisationen der Leistungserbringer auf Bundesebene,
- Stellen zur Gesundheitsberichterstattung (Statistik, Bund und Länder),
- Einrichtungen unabhängiger wissenschaftlicher Forschung (incl. Hochschulen),
- gemeinsamer Bundesausschuss (gBA)
- Institut für Qualität und Wirtschaftlichkeit im Gesundheitswesen (IQWiG),
- Institut des Bewertungsausschusses (InBA),
- Patienten- und Behindertenbeauftragte (Bund, Länder),
- Institut für Qualitätssicherung und Transparenz im Gesundheitswesen (IQTIG),
- Institut für das Entgeltsystem im Krankenhaus (INEK GmbH),
- Oberste Bundes- und Landesbehörden (also z.B. das BMG),
- Bundeskammern der Ärzte, Zahnärzte, Psychotherapeuten und Apotheker,
- Deutsche Krankenhausgesellschaft (DKG).

Gegenüber dem bisherigen Rechtszustand wurde die Empfangsbefugnis um öffentlich geförderte **außeruniversitäre Forschungseinrichtungen** ergänzt, also z.B. die Fraunhofer Gesellschaft, die Helmholtz Gesellschaft, die Leibniz Gemeinschaft sowie die Max-Planck-Gesellschaft.[17] Nicht Gesetz wurde der weitergehende Vorschlag der FDP im Gesundheitsausschuss, auch den pharmazeutischen Unternehmen, den Herstellern von Medizinprodukten, den Herstellern von Diagnostikleistungen und von digitalen Gesundheitsleistungen Zugang zu den Transparenzdaten einzuräumen. Dieser Vorschlag wurde von CDU/CSU, SPD, Die Linke und Bündnis 90/Die Grünen abgelehnt.[18]

Als Nutzungszwecke werden in § 303e Abs. 2 aufgeführt:

- Steuerungsaufgaben durch die Kollektivvertragspartner (Nr. 1),
- Verbesserung der Versorgungsqualität (Nr. 2),
- Planung von Leistungsressourcen (z.B. Krankenhausplanung, Nr. 3),
- Unterstützung politischer Entscheidungen (Nr. 5),
- Analyse und Entwicklung sektorenübergreifender Versorgungsformen und von Krankenkassen-Einzelverträgen (Nr. 6),
- Gesundheitsberichterstattung (Nr. 7).

Als weiterer Nutzungszweck wird die Forschung genannt (Nr. 4).

Für diese Zwecke liefert das Forschungsdatenzentrum Auswertungen „**anonymisiert und aggregiert**". Möglich ist auch die Lieferung „mit kleinen Fallzahlen", wenn nachvollziehbar dargelegt wird, dass dies für einen zulässigen Nutzungszweck (s.o.) erforderlich ist (§ 303e Abs. 3).

Datenschutzrechtlich besonders sen-

sibel wird es, wenn das Forschungsdatenzentrum **pseudonymisierte Einzeldatensätze** bereitstellt. Dafür muss der Antragsteller darlegen, dass dies „für einen nach Absatz 2 zulässigen Nutzungszweck, insbesondere für die Durchführung eines Forschungsvorhabens, erforderlich ist“. Die Pseudonyme werden bei der Bereitstellung nicht sichtbar gemacht. Zudem muss der Nutzer „einer Geheimhaltungspflicht nach § 203 des Strafgesetzbuchs unterliegen“ (bzw. gemäß Verpflichtungsgesetz) und technisch-organisatorisch gewährleisten, dass keine Kopien angefertigt werden und Datenminimierung praktiziert wird (§ 303e Abs. 4).

In der **Begründung** wird das Vorgehen wie folgt erläutert: „Die Regelung verbessert die Zugangsmöglichkeiten zu Einzeldatensätzen unter Kontrolle des Forschungsdatenzentrums. Einzeldatensätze werden nicht an Nutzungsberechtigte übermittelt. Wenn erforderlich und sicher umsetzbar, ist ein Zugriff auf Einzeldatensätze für die Verarbeitung unter Kontrolle des Forschungsdatenzentrums, insbesondere zur Analyse und zur Herstellung von zusammengefassten Daten möglich und kommt nicht mehr nur als Ausnahmefall in Betracht. Es kann dennoch in vielen Fällen weiterhin ausreichend sein, wenn ohne einen Zugriff auf Einzeldatensätze aufbereitete aggregierte Daten übermittelt werden. …

Als geeignete Verfahren … kommt der Zugriff an einem Gastarbeitsplatz in den Räumen des Forschungsdatenzentrums oder über einen **gesicherten Fernzugriff** in Frage. Hierfür stellt das Forschungsdatenzentrum eine geeignete technische Analyseplattform zur Verfügung. Bei der Entwicklung, Erprobung und Festlegung der Verfahren ist das Bundesamt für die Sicherheit in der Informationstechnik einzubeziehen, um ausreichende technische Sicherheit zu gewährleisten“.[19]

Die Nutzungsberechtigten dürfen die erlangten Daten nur **für die genehmigten Zwecke nutzen** und nicht an Dritte weitergeben, es sei denn, dass dies vom Forschungsdatenzentrum genehmigt wird. Sie haben „darauf zu achten, keinen Bezug zu Personen, Leistungserbringern oder Leistungsträgern herzustellen. Wird ein Bezug zu Personen, Leistungserbringern unbeabsichtigt hergestellt, so ist dies dem Forschungsdatenzentrum zu melden“. Die Nutzung zwecks Identifizierung von Leistungserbringern sowie zur Erlangung von fremden Betriebs- und Geschäftsgeheimnissen wird verboten (§ 303e Abs. 5).

Stellt eine Datenschutzaufsichtsbehörde einen **Datenschutzverstoß** fest und hat sie eine Maßnahme nach Art. 58 Abs. 2 lit. b-j DSGVO ergriffen, dann informiert sie das Forschungsdatenzentrum, das dann die Person bzw. Stelle für einen Zeitraum von bis zu zwei Jahren vom Datenzugang ausschließt.

§ 303a Abs. 4 ermächtigt das BMG in Abstimmung mit dem Bundesforschungsministerium (BMBF) zwecks Konkretisierung der Verfahren (Datenumfang, Pseudonymisierungsverfahren, Bereitstellung von Einzeldatensätzen, Aufbewahrungsfrist, Evaluation, Weiterentwicklung) zum Erlass einer **Rechtsverordnung**. Gemäß § 303d Abs. 2 wird ein Arbeitskreis der Nutzungsberechtigten eingerichtet, der „an der Ausgestaltung, Weiterentwicklung und Evaluation des Datenzugangs“ beratend mitwirkt.

3 Was davon zu halten ist

Es stimmt, dass im Forschungsdatenzentrum eine **zentrale Datensammlung von hochsensiblen Gesundheitsdaten** von sämtlichen in Deutschland gesetzlich Versicherten auf- bzw. ausgebaut wird. Dies ist ein höchstsensibler Vorgang, der einer qualifizierten Überprüfung und Hinterfragung bedarf. Es trifft aber nicht zu, dass, wie von vielen Kritikern suggeriert wird, damit dem Missbrauch dieser Daten Tür und Tor geöffnet wird. Dafür sind die Vorkehrungen, oder wie die DSGVO sagt, die „angemessenen und spezifischen Maßnahmen zur Wahrung der Rechte und Freiheiten“, zu klar und präzise. Dennoch bestehen rechtliche und voraussichtlich auch praktische Defizite, was mit großer Wahrscheinlichkeit zu Konflikten und möglicherweise auch zu unerwünschten Datenlecks führen wird.

Vorab soll aber klar gestellt werden: Die Nutzung der GKV-Gesundheitsdaten für Forschungszwecke ist äußerst sinnvoll, wenn diese zur **Weiterentwicklung unseres Gesundheitssystems** und zum Fortschritt im Bereich der medizinischen Forschung genutzt werden. Ohne valide statistische Daten, die im medizinischen Bereich äußerst differenziert sein müssen, ist eine qualifizierte Gesundheitsberichterstattung nicht möglich.[20] Diese ist nötig als Grundlage für eine gerechte und effiziente staatliche Politik, für die Justierung des Abrechnungssystems, für das Erkennen von grundlegenden Entwicklungen und Zusammenhängen.[21] Angesichts der Bedeutung der Medizin für unsere älter werdende Gesellschaft und angesichts gesteigerter Gesundheitsgefahren etwa durch ökologische Risiken und angesichts der hohen hier eingesetzten gesellschaftlichen Aufwände ist eine umfassende Datenbasis für Forschungszwecke wichtiger denn je.

Zugleich ist das **Recht auf informationelle Selbstbestimmung** und damit die individuelle Souveränität der Patientinnen und Patienten über ihre Daten ein hohes verfassungsrechtliches Gut. Dieses kann nur im überwiegenden Allgemeininteresse beschränkt werden, wenn hinreichende technisch-organisatorische und verfahrensrechtliche Vorkehrungen getroffen werden.[22]

Von Datenschützern wurde die uneingeschränkte Zugriffsmöglichkeit vieler Stellen kritisiert, ohne dass ein **Widerspruchsrecht** gegen die Datennutzung für Forschungszwecke vorgesehen ist.[23] Im deutschen Datenschutzrecht hat bei Forschungsnutzungen die Einwilligung absoluten Vorrang.[24] Dem gegenüber ist Art. 5 Abs. 1 lit. b DSGVO, der eine grundsätzliche und generelle Erlaubnis einer Zweitnutzung für Forschungszwecke vorsieht, erheblich forschungsfreundlicher, indem die DSGVO zwar Garantien für die Betroffenen fordert, nicht aber deren Zustimmung. Hintergrund dieses Schwenks ist, dass das Einwilligungserfordernis ebenso wie eine Widerspruchsmöglichkeit die Repräsentativität von wissenschaftlichen Auswertungen beeinträchtigen kann. Für einen Ausgleich zwischen Forschungsfreiheit und Datenschutz ist eine generelle Widerspruchsmöglichkeit nicht zwingend, wenn andere Vorkehrungen den Betroffenenschutz sichern. Ein Minus dazu könnte eine erhöhte Transparenzpflicht gepaart mit einem projektspezifischen Widerspruchsrecht sein.[25] Tatsächlich ließe sich damit eine erheblich differenziertere Umsetzung des Rechts auf

informationelle Selbstbestimmung bei gleichzeitiger hoher Repräsentativität sichern. Gerade bei der Auswertung von Einzeldatensätzen wird das Spannungsverhältnis zwischen Datenschutz und Forschungsnutzung virulent. Dass den Betroffenen bei der Datentransparenz im DVG überhaupt keine Rechte zugestanden werden, ist definitiv ein zentraler Aspekt, um die Regelungen zur Datentransparenz rechtlich anzugreifen.

Hinsichtlich der **Datennutzungsrechte** nennt das Gesetz eine Vielzahl von Stellen. Für die meisten genügen aggregierte, also vollständig anonymisierte Auswertungsergebnisse, etwa für die Krankenhausgesellschaft oder sonstige GKV-Verbände. Diese Stellen werden im Gesetz mit Forschenden in eine Reihe gestellt, die viele ihrer Fragestellungen sicher nur mit personenbeziehbaren Einzeldatensätzen beantworten können. Dies mag gesetzgebungstechnische Gründe haben, also das Ziel einer möglichst schlanken Regelung. Zugleich öffnet aber der Gesetzestext die Tür für die Übermittlung von Einzeldatensätzen an Stellen, die diese nicht erhalten dürfen. In der Praxis bzw. durch Rechtsverordnung muss gewährleistet werden, dass trotz der gesetzlichen Offenheit der Grundsatz der Datenminimierung nicht missachtet wird.

Das Problem des DVG ist, dass dieses nicht nur aggregierte Auswertungen mit anonymisierten Ergebnissen zulässt, sondern auch die Nutzung von **Einzeldatensätzen**, wenn nachvollziehbar dargelegt wird, dass diese für einen zulässigen Nutzungszweck erforderlich sind. Die Hürden für die Weiternutzung der Einzeldatensätze sind dann denkbar niedrig: 1. Die Empfänger müssen einer beruflichen Schweigepflicht unterliegen. 2. Die Datenminimierung muss technisch-organisatorisch abgesichert werden. 3. Es besteht eine Zweckbindung, die aber mit Genehmigung des Forschungsdatenzentrums aufgehoben werden kann. 4. Es besteht ein Reidentifizierungsverbot (§ 303e Abs. 4, 5). Eine saubere Abschottung, also eine räumliche, organisatorische und personelle Trennung zwischen der Erfüllung der operativen Aufgaben einer Stelle und der pseudonymen Verarbeitung von Transparenzdaten[26] ist ebensowenig vorgesehen wie sonstige Vorkehrungen gegen eine Reidentifizierung der pseudonymen Daten.[27]

Eine Sicherheitsvorkehrung soll darin bestehen, dass eine Auswertung der für den jeweiligen Nutzenden freigeschalteten Einzeldatensätze nur auf dem IT-System des Forschungszentrums zulässig ist. Damit verbindet die Gesetzesbegründung die unzutreffende Behauptung, so erfolge rechtlich keine Datenübermittlung.[28] Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) soll die ausreichende technische Sicherheit der technischen **Analyseplattform des Forschungsdatenzentrums** gewährleisten. Hier sind Fragezeichen bzgl. der Praktikabilität angebracht: Letztlich muss der Forschende bestimmte personenbeziehbare Daten mitnehmen, um sie weiter auswerten zu können. Forschende Fragestellungen werden regelmäßig nicht nur mit Transparenzdaten gemäß dem DVG bearbeitet werden; weitere Daten, etwa aus dem klinischen Bereich müssen einbezogen werden können. Zu einem Aufspielen solcher Daten auf dem System des Forschungsdatenzentrums wie für eine Mitnahme von personenbeziehbaren Datensätzen macht der Gesetzestext keine Aussage. Vielmehr hat die Bundesregierung die nachvollziehbare Forderung des Bundesrats, eine Verknüpfung der Datentransparenz mit „bereits existierenden Langzeitdatenbanken" zu ermöglichen mit dem wenig tragfähigen Argument zurückgewiesen, dies entspräche nicht „dem Gedanken der §§ 303a ff. SGB V, wonach nur Ergebnisse anhand der von den Nutzungsberechtigten beantragten Auswertungen an die Nutzungsberechtigten übermittelt werden und keine Vervielfältigung des umfangreichen Datenbestands erfolgen soll".[29]

Die Achillesferse, also der wohl verletzlichste Punkt bei der Datentransparenz aus Datenschutzsicht, ist, wie das **„spezifische Reidentifikationsrisiko** in Bezug auf die durch Nutzungsberechtigte nach § 303e beantragten Daten zu bewerten" ist. Diese Bewertung soll das Forschungsdatenzentrum durchführen (§ 303d Abs. 1 Nr. 5). Wird hier unsauber gearbeitet, so drohen Datenleaks. Wie diese Bewertung erfolgt, bedarf einer dauernden Hinterfragung, Transparenz und einer wissenschaftlichen Begleitung. Es handelt sich hier um Wesentliches, was nicht dem Verordnungsgeber überlassen werden kann (so aber § 303a Abs. 4 Nr. 4).

Die Vertraulichkeit ist nicht ausreichend gewährleistet: Der Verweis auf die **berufliche Schweigepflicht** ist materiell-rechtlich richtig und sinnvoll. Prozedural ist er absolut unergiebig: § 203 StGB hat als Sanktionsinstrument derzeit in der Praxis keine bzw. nur symbolische Bedeutung; Ermittlungen sind selten; Sanktionierungen sind die absolute Ausnahme.[30] Es ist nicht zu vermuten, dass die versteckte Sanktionsvorschrift in § 307b SGB V, der die Strafbarkeit z.B auf die bewusste Verschaffung von Kenntnissen über fremde Betriebs- und Geschäftsgeheimnisse ausweitet, größere Relevanz erhält.

Problematisch ist weiterhin, dass **keinerlei Kontrollmechanismen** vorgesehen sind. Es gelten lediglich die allgemeinen Regelungen der DSGVO, ohne dass spezifische Vorkehrungen getroffen werden. Diese könnten in Berichtspflichten, in der Etablierung eines spezifischen Kontrollgremiums, das z.B. regelmäßig Stichprobenprüfungen durchführt, und in spezifischen Sanktionsmechanismen liegen.

Dieses Defizit wird auch nicht durch eine verstärkte **Datenschutzkontrolle** kompensiert. Bei hochsensitiven, zentralisierten hoheitlichen Formen der Datenverarbeitung, die keinen sonstigen öffentlichen Kontrollmechanismen oder einer hinreichenden Transparenz unterliegen, hat das BVerfG gegenüber dem generellen Aufsichtsinstrumentarium verstärkte Maßnahmen gefordert, etwa kontinuierliche Regelkontrollen.[31]

Da hier keine besonderen Geheimhaltungsnotwendigkeiten bestehen, sind zusätzliche, nicht unbedingt auf den Einzelfall bezogene **Transparenzmaßnahmen** möglich und zwecks Schaffung angemessener Vorkehrungen auch nötig.[32] Das im Grundsatz zu begrüßende öffentliche Antragsregister (§ 303d Abs. 1 Nr. 6)[33] ist für eine wirksame Hinterfragung mit Angaben zu Nutzungsberechtigten, Vorhaben und deren Ergebnissen ungeeignet, solange nicht erkennbar ist, inwieweit welche Einzeldatensätze von den Nutzenden verarbeitet wurden.

Der Bundesrat hat das Kontrollproblem erkannt und zumindest gefordert, dass Anträge auf Datenzugang neutral

zu entscheiden sind und eine unabhängige Kontrolle zu gewährleisten ist. Die Bundesregierung und die Bundestagsmehrheit sahen hierfür keine Notwendigkeit: „Das Forschungsdatenzentrum ist eine öffentliche Stelle des Bundes, das der Rechtsaufsicht des Bundesministeriums für Gesundheit untersteht."[34] Im BMG besteht aber leider weder hinreichendes Problembewusstsein, geschweige denn die fachliche Kompetenz, dieser hochsensiblen Kontrollaufgabe nachzukommen.

Ein in der gesamten deutschen Rechtsordnung bestehendes Problem wird auch im DVG fortgeschrieben: Der Gesetzgeber hat völlig offengelassen, was überhaupt alles zur **zugangsprivilegierten Forschung** zu zählen ist. Zwar hat das BVerfG eine Definition gegeben. Danach ist Forschung ein auf wissenschaftlicher Eigengesetzlichkeit (Methodik, Systematik, Beweisbedürftigkeit, Nachprüfbarkeit, Kritikoffenheit, Revisionsbereitschaft) beruhender Prozess zum Auffinden von Erkenntnissen, ihrer Deutung und ihrer Weitergabe. Wissenschaftliche Forschung ist „alles, was nach Inhalt und Form als ernsthafter, planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist".[35] Doch kann diese Definition nicht ausreichen, um den Umgang mit personenbezogenen Daten hinreichend zu begrenzen und grundrechtskonform zu gestalten. Hierfür bedarf es spezifischer Regeln und Verfahren.[36] Die erste Gelegenheit, solche vorzusehen, nämlich die Umsetzung der DSGVO, haben die deutschen Gesetzgeber unerledigt vorbeiziehen lassen. Augenscheinlich ist der Leidensdruck gerade bei der medizinischen Forschung immer noch nicht groß genug, um auf die Politik überzuspringen. Für den Zugang zu den GKV-Transparenzdaten verlangt das DVG nicht mehr, als dass die Forschung öffentlich gefördert wird. Dabei handelt es sich ausschließlich um eine finanzielle Erwägung, bei welcher der Grundrechtsschutz gar keine Rolle spielt und ein öffentliches Interesse (der Institution, nicht des konkreten Projekts) allenfalls zu vermuten ist. Aus Sicht des Grundrechtsschutzes ist es dagegen nötig, dass Anforderungen an die Unabhängigkeit, die Transparenz, die Sicherungsvorkehrungen und das öffentliche Interesse des konkreten Projektes gestellt werden und diese im Rahmen eines administrativen Vorgangs geprüft, festgestellt und evtl. sanktioniert werden. Derartige Anforderungen könnten dann von der medizinischen Forschung auf die Forschung generell übertragen werden.

Die Gesetzgeber haben sich in Deutschland bisher noch keine strukturierten Gedanken über die datenschutzrechtliche Regulierung von Forschung gemacht. Die Umsetzung der DSGVO hat insofern bisher keine Wende gebracht.[37] Das zeigt sich nun auch beim DVG, bei dem unklar bleibt, wie die §§ 303a-303f SGB V im **Verhältnis zu sonstigen SGB-Forschungsregelungen** stehen. So werden Krankenkassen und den Kassenärztlichen Vereinigungen, die auch nach § 303e Abs. 1 Nr. 3 u. 4 berechtigt sind, in § 287 SGB V begrenzte Forschungsauswertungen erlaubt. Ob § 287 ergänzend oder alternativ anwendbar ist, ist offen. In verstärktem Maß stellt sich die Frage nach dem Verhältnis der Forschungsspezialregelungen zueinander bei den §§ 67c Abs. 2 Nr. 2, Abs. 5, 75 Abs. 1, 2 oder 4a Satz 1 SGB X. Darin erfolgen Zweckbeschränkungen für Forschende auf den „Sozialleistungsbereich", auf „Arbeitsmarkt- und Berufsforschung" oder auf Projekte, die zum ursprünglichen Vorhaben zumindest „in einem inhaltlichen Zusammenhang" stehen. Diese pauschalen Zweckbeschränkungen dürften gegen die generelle Forschungsprivilegierung bei einer Sekundärnutzung nach Art. 5 Abs. 1 lit. b DSGVO verstoßen. Es handelt sich aber um geltendes Recht. Ob damit der in § 303e Abs. 2 Nr. 4 genannte generelle Zweck „Forschung" eingeschränkt wird, müsste man gemäß dem Grundsatz, dass die speziellere die allgemeinere Regelung verdrängt, annehmen.

4 Fazit

Das Digitale-Versorgung-Gesetz ist mit seinen Regelungen zur Datentransparenz gut gemeint, aber schlecht gemacht. Es gibt sich nominal viel Mühe, Vorkehrungen zum Datenschutz zu treffen. Dabei fällt auf, dass insbesondere technische Maßnahmen vorgesehen sind. Das Instrument der Pseudonymisierung wird als Generalwaffe zur Verhinderung des individualisierten Datenmissbrauchs in Stellung gebracht. Dieser im Grunde richtige Ansatz wird aber dadurch konterkariert, dass für diesen technischen Schutz **kein administrativer Unterbau** geschaffen wird. Das Verfahren der Pseudonymisierung generell wie im einzelnen Projektfall setzt Kompetenz, Dokumentation, Erprobung und Kontrolle voraus. Das kostet alles Geld. Vielleicht war dies der Grund, weshalb man hierzu keine Klärung herbeiführen wollte. Dieses Defizit rächt sich, wenn letztlich das BVerfG oder der EuGH feststellen sollte, dass die technisch-organisatorischen und prozeduralen Anforderungen ungenügend für den Grundrechtsschutz der GKV-Versicherten sind. Damit würde dem berechtigten Anliegen, eine bessere Datenbasis für die medizinische Forschung zu schaffen, ein Bärendienst erbracht.

Kritikwürdig ist auch die **systematische Stellung der Regeln** zur Datentransparenz im DVG: Solange bei der Datenverarbeitung noch der Risikostrukturausgleich im Vordergrund stand, mag eine Regulierung im SGB V „unter ferner liefen..." noch gerechtfertigt gewesen sein. Diese Stellung wird aber der nun massiv gesteigerten Bedeutung nicht mehr gerecht. Das SGB ist ohnehin nicht für Normalverbraucher, ja selbst für Juristen kaum lesbar und verständlich. Durch ein eigenständiges Gesetz ohne die vierstellige Bezifferung von 303a bis 303f hätte dieses Defizit zumindest ein wenig behoben werden können.

Nicht verständlich ist, mit welcher Unkenntnis die Politik immer noch mit den Bedürfnissen medizinischer Forschung und den bestehenden rechtlichen Möglichkeiten und Notwendigkeiten umgeht. So stellt sich schon die Frage, ob die umfassende **Zweckprivilegierung** des Art. 5 Abs. 1 lit. b DSGVO für Statistik und Forschung hier korrekt umgesetzt wurde. Diese Frage muss man jedenfalls verneinen, wenn man die weiteren im SGB geltenden Forschungsregelungen, die durch das DVG nicht ausgeschlossen sind, anwendet.

Nicht praktikabel dürfte sich die Nutzung der Datentransparenz für die universitäre Forschung erweisen, bei der es um ein **Verschneiden von Klinikdaten mit GKV-Daten** geht. Hieraus könnten auch wichtige Rückschlüsse gezogen

werden auf finanzbedingte Umgehungsstrategien bei der GKV-Abrechnung. Jenseits dieses hochverminten Gebietes gibt es aber auch epidemiologisch sinnvolle und wichtige Ansätze eines solchen Verschneidens, die mit dem vorliegenden DVG nicht ermöglicht werden.

Das Digitale-Versorgung-Gesetz ist nun mal in Kraft. Seine Umsetzung muss jetzt aufmerksam, fachkundig und **kritisch begleitet** werden. Das Problembewusstsein hierfür scheint an vielen Stellen noch zu fehlen. Dieses fehlende Bewusstsein kann zwei Irrwege zur Folge haben: Die Datentransparenz verharrt weiter in ihrem bisherigen Dornröschenschlaf mit der Folge, dass wichtige Fragestellungen in der Medizinforschung weiterhin unbeantwortet bleiben. Zu befürchten ist aber viel mehr, dass sich eine intransparente Nutzungspraxis entwickelt, bei der letztlich das Grundrecht der Betroffenen auf Datenschutz auf der Strecke bleibt. Dies muss verhindert werden. Wirksam verhindert werden kann dies nur dadurch, dass bei dem Gesetz nachgebessert wird.

1 G. v. 09.12.2019, BGBl. I S. 2562.

2 Stadler, Digitaler Tinnitus, SZ 08.11.2019, 7.

3 Krempl, Bundestag für Apps auf Rezept und zentrale Datenauswertung, www.heise.de 07.11.2019, Kurzlink: https://heise.de/-4582028

4 G. v. 14.11.2003, BGBl. I S. 2190, grundlegend überarbeitet mit G. v. 22.12.2011, BGBl. I S. 2983. Werden im folgenden Text Paragraphen ohne Gesetzesbezeichnung genannt, so handelt es sich um solche des SGB V.

5 Weichert, DANA 4/1999, 22.

6 Stellungnahme Steven, Digitale Gesellschaft v. 10.10.2019, BT-Ausschuss f. Gesundheit, Ausschussdrucksache 19(14)105(7), S. 4.

7 Ludwig, Öffentlich krank, SZ 13.11.2019, 19.

8 Ludwig, Öffentlich krank, SZ 13.11.2019, 19; Krempl (En. 3).

9 Ludwig, Öffentlich krank, SZ 13.11.2019, 19.

10 Weichert ZD 2020, 20.

11 BT-Drs. 19/13438, S. 71.

12 BT-Drs. 19/13438, S. 72.

13 BT-Drs. 19/13438 S. 72; Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF), Stellungnahme v. 09.10.2019, BT-Ausschuss f. Gesundheit, Ausschussdrucksache 19(14)105(12), S. 4.

14 BT-Drs. 19/13438, S. 73.

15 TMF (En. 13), S. 5.

16 BT-Drs. 19/13438, S. 73.

17 BT-Drs. 19/13438, S. 74.

18 BT-Drs. 19/14867, S. 84 ff.

19 BT-Drs. 19/13438, S. 74.

20 Weichert, Big Data im Gesundheitsbereich, 2018, https://www.abida.de/sites/default/files/ABIDA%20Gutachten-Gesundheitsbereich.pdf, S. 45 f., 163 f.

21 BVerfG 15.12.1983 – 1 BvR 209/83 u.a. (Volkszählung), Rn. 105, NJW 1984, 423.

22 BVerfG 15.12.1983 – 1 BvR 209/83 u.a., LS. 2, NJW 1984, 419.

23 So z.B. PE Patientenrecht und Datenschutz e.V, 15.01.2020.

24 Weichert/Bernhardt/Ruhmann, Die Forschungsklauseln im neuen Datenschutzrecht, 18.10.2018, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2018_forschungklauseln_181018.pdf, S. 5.

25 Krawczak/Weichert, DANA 4/2017, 199.

26 BVerfG 15.12.1983 – 1 BvR 209/83 u.a., Rn. 109 ff., NJW 1984, 423.

27 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Stellungnahme vom 23.10.2019, S. 5.

28 BT-Drs. 19/13438, S. 74.

29 BT-Drs. 13/13548, S. 9.

30 Fischer, Strafgesetzbuch, 66. Aufl. 2019, § 203 Rn. 5.

31 BVerfG 24.03.2013 – 1 BvR 1215/07, Rn. 116 f. (Antiterrordateigesetz), NJW 2013, 1504.

32 Zur Transparenz bei Forschung Weichert ZD 2020, 20.

33 Ebenso TMF (En. 13), S. 5.

34 BT-Drs. 19/13548, S. 9.

35 BVerfGE 35, 112 f. = NJW 1978, 1176; Werkmeister/Schwaab CR 2019, 85; Roßnagel, ZD 2019, 158f.; ähnlich Art. 2 lit. b Richtlinie 2005/71/EG des Rates über ein besonderes Zulassungsverfahren für Drittstaatsangehörige zum Zweck der wissenschaftlichen Forschung v. 12.10.2005, zur Erfordernis der Staatsferne Weichert, Informationelle Selbstbestimmung und strafrechtliche Ermittlung, 1990, 231 f.; Britz in Dreier, GG Bd. I, 3. Aufl. 2013, Art. 5 III (Wissenschaft), Rn. 74 f.

36 Weichert ZD 2020, 23 f.

37 Weichert/Bernhardt/Ruhmann (En. 24).

Interview mit einem Arzt*

Datenschutz in der Klinik

Datenschutz im Krankenhaus – Gehen dadurch persönliche Kontakte verloren oder erhöht sich das Vertrauen in den Arzt?

Die Tatsache, dass in den Krankenhäusern Datenschutzrichtlinien existieren und Berücksichtigung finden, dürfte sich eher positiv auf das Arzt-Patient-Verhältnis auswirken. Der persönliche Kontakt von Patienten zu ihren behandelnden Ärzten und umgekehrt wird durch den Datenschutz jedenfalls nicht beeinträchtigt. Das Vertrauen in den Arzt ist aber in erster Linie auf dessen Fachkompetenz zurückzuführen. Inwieweit sich das Vertrauen zu den Ärzten erhöht in Kenntnis des Umstandes, dass in der Klinik generell Datenschutzrichtlinien existieren und umgesetzt werden, kann ich nicht sicher

beurteilen. Ich könnte mir aber sehr gut vorstellen, dass sich die Vertrauensbasis zueinander eher verstärkt, wenn ein Arzt dem Patienten zusätzlich das Gefühl vermittelt, diskret und sorgsam mit dessen Patientendaten umzugehen. Erfahrungsgemäß setzen Patienten voraus, dass mit ihren Daten vertrauensvoll umgegangen wird.

Welche Rolle spielt der Datenschutz im Verhältnis zu Angehörigen (insbesondere bei Kindern und alten Menschen)?

Es gehört zu den üblichen täglichen Aufgaben sowohl des ärztlichen, als auch des pflegerischen Personals, Familienangehörigen Auskünfte zu erteilen. Dies scheint aus Sicht der Angehörigen so selbstverständlich zu sein, dass man übersieht, dass Auskünfte gegenüber Familienangehörigen eigentlich der ärztlichen Schweigepflicht unterliegen. Wir Ärzte gehen stillschweigend von einer mutmaßlichen Einwilligung des Patienten aus, die vorsieht, dass der zu behandelnde Patient grundsätzlich damit einverstanden ist, dass seine engeren Angehörigen – zum Beispiel die Ehefrau oder die erwachsenen Kinder - über dessen Krankheitsverlauf in Kenntnis gesetzt werden. Und da in der Regel solche Gespräche mit Angehörigen immer im Beisein des Patienten stattfinden, darf ich als Arzt allgemein voraussetzen, dass die Einbeziehung von engeren Angehörigen in die Arztgespräche vom Patienten auch gewollt ist, es sei denn, er widerspricht eindeutig oder grenzt den Kreis derer, die informiert werden dürfen, im Vorfeld eindeutig ein. Telefonische Auskünfte werden nur den uns persönlich bekannten Angehörigen erteilt, um den Schutz der Privatsphäre zu gewährleisten. Telefonische Auskünfte an nicht bekannte Personen werden nicht erteilt.

Sofern minderjährige Kinder medizinisch behandelt werden müssen, erteilen wir den besorgten Eltern als ihren gesetzlichen Vertretern bereitwillig die notwendigen Auskünfte, insbesondere vor dem Hintergrund, dass die Kinder noch nicht einsichtsfähig sind. Meist sind wir auf die Eltern, allenfalls auch auf die Großeltern fokussiert und erteilen darüber hinaus niemandem Auskünfte. Es hat sich bewährt, Freunde und Bekannte darauf zu verweisen, sich bei den Eltern nach dem Gesundheitsverlauf minderjähriger Kinder zu erkundigen.

So notwendig und sinnvoll die Gespräche mit den Eltern von minderjährigen Kindern auch sein mögen, sie bedürfen streng genommen aus Sicht des Datenschutzes der Erlaubnis, weil auch die Behandlung von Kindern und die Weitergabe von Befunden durch die ärztliche Schweigepflicht geschützt und damit limitiert ist. Die weitläufig praktizierte Regelung sieht vor, dass Ärzte von einer mutmaßlichen Einwilligung ausgehen und damit Auskünfte an die Eltern zum Wohle ihres Kindes erteilen dürfen.

Auf wenig Verständnis dürfte die Tatsache stoßen, dass unter Berufung auf die ärztliche Schweigepflicht die Eltern von einsichtsfähigen Kindern im Gegensatz zu noch nicht einsichtsfähigen, jüngeren Kindern nicht selbstverständlich über den Behandlungsverlauf ihrer minderjährigen Kinder aufgeklärt werden, obwohl sie die gesetzlichen Vertreter ihrer Kinder sind. Um Verstöße gegen den Datenschutz zu vermeiden, müssten diese Jugendlichen hinsichtlich der Auskunftserteilung an ihre Eltern eigentlich streng genommen ihre Zustimmung erteilen. Ein solches Vorgehen ist für Eltern schwer nachvollziehbar.

Ältere Menschen vertreten sich üblicherweise selbst, sofern sie nicht in ihrer Entscheidungsfindung eingeschränkt sind. Wenn aufgrund körperlicher Gebrechen oder infolge einer zunehmenden Einschränkung der Hirnleistung im Sinne einer Altersdemenz oder anderer hirnorganischer Erkrankungen oder Schädigungen dies doch der Fall sein sollte, liegt in aller Regel eine Betreuung vor. Unter diesen Voraussetzungen sind wir primär gegenüber der von Amtswegen als Betreuer oder Betreuerin eingesetzten Person auskunftsberechtigt. Unter praktischen Gesichtspunkten ist in der Regel der Ehepartner oder ein erwachsenes Kind als Betreuer eingesetzt. Die Weitergabe von Auskünften an andere Angehörigen unterliegt Gesetzen des gesunden Menschenverstandes und erfolgt ohne Verletzung von Datenschutzrichtlinien.

Wie die Angehörigen mit diesen Informationen, die sie von Ärzten oder Pflegekräften erhalten und die wir üblicherweise pfleglich behandelt haben, dann letztendlich in der Öffentlichkeit umgehen, wissen wir meist nicht. Somit könnte sich eine Grauzone entwickeln, wenn Angehörige plötzlich innerhalb des Familienkreises, innerhalb des Freundeskreises oder auch sonst in der Öffentlichkeit Informationen preisgeben, die wir eigentlich nicht für die Öffentlichkeit gedacht hatten. Auch wenn wir uns ärztlicherseits datenschutzkonform verhalten, könnte der Datenschutz durch zu freizügigen Umgang mit Patientendaten durch Angehörige gewissermaßen unterlaufen werden.

Anders muss der Fall bewertet werden, wenn ein behandelnder Arzt von einem Freund oder Bekannten eines Patienten angesprochen und um Auskunft über dessen Krankheit gebeten wird. Er müsste in diesem Fall konkret unter Berufung auf die ärztliche Schweigepflicht darauf verweisen, dass er keine Auskünfte erteilen darf. Der Arzt darf nur dann Auskünfte erteilen, wenn er ausdrücklich vom Patienten dazu legitimiert worden ist.

Aus Gründen des Datenschutzes geben wir zu Beginn der medizinischen Behandlung grundsätzlich keine telefonischen Auskünfte an Personen, die wir nicht kennen, bzw. die wir dem Patienten gegenüber nicht zuordnen können. Ich erwarte, dass sich eine dem Patienten nahestehende Person persönlich vorstellt, damit ich weiß, welche persönliche Beziehung zum Patienten vorliegt und ob mit Einverständnis des Patienten Auskünfte erteilt werden dürfen, ohne die ärztliche Schweigepflicht oder den Datenschutz zu verletzen. Im Laufe der Behandlung entwickelt sich meist ein gewisses Vertrauensverhältnis zu den Patienten und deren Angehörigen, so dass gewährleistet ist, dass hier den richtigen Personen Auskünfte erteilt werden.

Fremden Personen, zum Beispiel Freunden oder sonstigen Bekannten (also nicht Angehörigen), werden keine Auskünfte erteilt. Dies kann nur erfolgen, wenn wir dazu mündlich oder schriftlich ausdrücklich legitimiert werden.

Aufklärung: Im Web und bei App-Nutzung stimmt man ja bedenkenlos allen Erklärungen zu (auch wenn sie nicht gelesen wurden) – Wie ist das im Krankenhaus?

Meine persönlichen Erfahrungen sind leider die, dass die Einstellung der Patienten hinsichtlich der von ihnen mit Unterschrift genehmigten Erklärungen und Aufklärungen im Krankenhaus nicht viel anders ist als im Alltagsleben. Dabei hängt doch so viel davon ab. Der Patient nimmt sich häufig nicht die Zeit, im Vorfeld den Aufklärungsbogen durchzulesen, um etwas informierter und vorbereiteter mit dem Arzt das wesentliche Gespräch über eine bevorstehende und notwendige medizinische Maßnahme zu führen. Aufklärungsgespräche werden in guter Absicht und immer zweckgebunden geführt, um einem Patienten einen von ärztlicher Seite vorgeschlagenen einwilligungspflichtigen medizinischen Eingriff zu verdeutlichen. Aufklärungsgespräche dienen nicht zuletzt auch der rechtlichen Absicherung eines bevorstehenden medizinischen Eingriffs, denn das Unterlassen einer Aufklärung bzw. die nicht erfolgte Einwilligung des Patienten erfüllt streng genommen den Tatbestand der Körperverletzung. Es ist die Aufgabe des Arztes, den Patienten so aufzuklären, dass dieser am Ende der Aufklärung nicht nur die Aussagen des Arztes inhaltlich verstanden hat, sondern in die Lage versetzt wird, abzuwägen, welche Entscheidung für ihn die Richtige ist. Bevor er unterschreibt, muss der Patient nach dem Gespräch entscheiden können, ob er sich tatsächlich - so wie von ärztlicher Seite vorgeschlagen - behandeln lässt, eingedenk der Risiken und Komplikationen, die auf ihn zukommen könnten, aber auch eingedenk des Nutzens, der mit einer Behandlungsmaßnahme verbunden sein kann.

Leider werden diese Aufklärungsgespräche in der heutigen Zeit der Arbeitsverdichtung im Eiltempo und mitunter auch oberflächlich durchgeführt, so dass der Patient sie inhaltlich nicht vollständig verstehen kann. Auch gelingt es den Ärzten nicht immer, Zweifel beim Patienten auszuräumen. Wenn man die Aufklärung mit dem Patienten optimal durchführen will, muss man ihm nach der Aufklärung auch die Möglichkeit lassen, sich Gedanken zu machen. Er braucht eine entsprechende Bedenkzeit, um abwägen zu können, ob er die Behandlungen auch wirklich durchführen lassen will.

Ich möchte einen Patienten nicht vorverurteilen und ihn auch nicht für gleichgültig erklären, wenn er ohne Nachfrage oder kritiklos seine Unterschrift unter einen Aufklärungsbogen für eine medizinische Behandlung setzt. Meine Wahrnehmung ist die, dass Patienten sich häufig darauf verlassen, dass die Ärzte schon das Richtige für sie tun werden.

Einsichtnahme: Privatpatienten kommen eher an ihre Daten/Befunde etc. als Kassenpatienten – Stimmt das?

Bis zu einem gewissen Grade dürfte dies wohl auch stimmen. Der Hauptgrund dürfte wohl der sein, dass der Privatpatient für seine Leistung mehr bezahlt als der Kassenpatient. Ich kann nachvollziehen, dass der behandelnde Arzt aus diesem Grund eher bereit ist, dem Privatpatienten die eine oder andere Gefälligkeit zu erweisen. Wenn dieser einen Auszug aus seiner Krankenakte haben möchte, ist man geneigt, dem Privatpatienten dies eher zuzubilligen als einem Kassenpatienten. Eines muss man in diesem Zusammenhang aber klarstellen: Beide, Privat- wie Kassenpatient, haben das gleiche Recht auf Einsicht in die Krankenakte und auf die Aushändigung von Auszügen aus der Krankenakte. Es ist insofern nicht gerechtfertigt, den Privatpatienten vorzuziehen und den Kassenpatienten zu benachteiligen. Auch ein Kassenpatient darf sich Auszüge aus seiner Krankenakte kopieren lassen, die er für seinen eigenen Gebrauch oder für zukünftige Behandlungen reservieren lassen darf. Eine Weigerung des Arztes käme einer Diskriminierung gleich.

Die tägliche Arbeit: Ist der Datenschutz ein Hindernis und wenn ja, wodurch?

In der täglichen Arbeit empfinde ich den Datenschutz nicht als Hindernis, weil er Teil meines Handelns geworden ist. Wir wissen alle, dass wir mit den Daten unserer Patienten behutsam umgehen müssen und richten uns in aller Regel danach. Die Berücksichtigung des Datenschutzes ist einer etablierten Fehlerkultur in einem Unternehmen vergleichbar und zielt darauf ab, die eigenen täglichen Handlungen zu optimieren und sie nahezu fehlerfrei zu gestalten. Dennoch unterstelle ich, dass jeder von uns in Situationen kommt, in denen wir oberflächlicher mit den Daten umgehen, anstatt uns streng datenschutzkonform zu verhalten. Auch kennen wir die Datenschutzrichtlinien nicht in- und auswendig, so dass Überschreitungen durchaus, wenn auch ungewollt, vorkommen könnten.

Andererseits sind unsere Handlungsspielräume schon recht umfangreich gestaltet, die durch Datenschutzrichtlinien nicht eingeschränkt werden. Gerade im medizinischen Bereich muss ein umfassender, kontrollierter Datenaustausch zwischen Ärzten, Pflegekräften und sonstigem medizinischen Hilfspersonal zum Zwecke einer sachgerechten Behandlung der Patienten möglich sein. Die Verpflichtung des Arztes, die im Vertrauen geäußerten Geheimnisse des Patienten nicht weiterzugeben, schränkt den Austausch von Daten grundsätzlich nicht ein, sofern dieser fach- und sachbezogen erfolgt. Auf diese Weise werden Konsiliarbehandlungen zwischen Abteilungen oder Anschlussbehandlungen durch eine andere Abteilung im selben Klinikum erst möglich. Auch müssen Recherchen in den Informationsdateien möglich sein, sofern sie fallbezogen der Informationsgewinnung durch Einsicht in frühere Behandlungsakten eines Patienten dienen.

Hingegen ist das ziellose Surfen in den Informationsdateien des Krankenhauses ebenso wenig erlaubt wie das Aufrufen von Krankenakten, die den „Suchenden" eigentlich nicht zu interessieren haben. Es ist unzulässig, dass jemand beispielsweise „rein zufällig" den Namen einer Person des öffentlichen Lebens in den Krankenakten findet und dann einmal nachschaut, woran diese Person erkrankt sein mag. Damit verstößt man eindeutig gegen Datenschutzrichtlinien und verletzt die Privatsphäre des betreffenden Patienten. Unabhängig davon, ob diese Person berühmt ist oder nicht, liegt im vorliegenden Fall kein medizinisches Interesse vor. Ein solches unbefugtes Eindringen in die Privatsphäre wird in unserem Krankenhaus, das über einen Datenschutzbeauftragten verfügt,

geahndet, weil das unbefugte Surfen in den Patientendateien in unserem Haus untersagt ist und deshalb zur Vermeidung eines Missbrauchs auch systemimmanent erfasst wird.

„Halbgott in Weiß“ – Gibt es den noch? Konkreter: Muss ein Arzt alles über den Patienten wissen? Müssen alle Ärzte alles wissen?

Es gibt auch heute sicher immer noch Mediziner, die – meist in leitender Position – von sich selbst so sehr überzeugt sind, dass das Vorurteil eines sprichwörtlichen „Halbgottes in Weiß“ weiter bestehen bleibt. Diesem werden Attribute wie Unnahbarkeit, Arroganz oder Überheblichkeit unterstellt. Meine subjektive Wahrnehmung ist die, dass Kolleginnen oder Kollegen dieser Prägung im täglichen Umgang zwar sehr anstrengend sein können, aber interessanterweise häufig über eine überdurchschnittliche fachliche Qualifikation verfügen. Diese Widersprüchlichkeit ist schon auffallend. Ich gehe dennoch davon aus, dass diese Spezies langsam, aber sicher aussterben wird.

Die Frage, ob ein behandelnder Arzt „seinen“ Patienten auf der Grundlage medizinischer Fakten kennen muss, muss ich konkret mit einem eindeutigen „ja“ beantworten. Ich erwarte, dass ein behandelnder Arzt über seinen Patienten detailliert informiert ist, insbesondere dann, wenn er ihn persönlich behandelt. Dies schließt seine aktuelle Krankengeschichte, frühere Behandlungsverläufe, sein soziales Umfeld, seine familiäre Situation mit ein. Ich erwarte auch, dass mittels Recherche in den krankenhausinternen Netzwerken Informationen über den Patienten einholt werden, die letztendlich notwendig sind, um einen erfolgreichen Behandlungs- und Heilungsprozess einzuleiten.

Die Frage, ob alle Ärzte alles wissen müssen, möchte ich wie folgt beantworten: Viele Ärzte haben ein überdurchschnittliches Wissen über medizinische Krankheitsbilder angehäuft, das im Zuge der Behandlung unserer Patienten sicher sehr hilfreich ist. Aber auch wenn man nicht alles weiß, so wie zu Beginn einer medizinischen Ausbildung, ist das Nachschlagen von Fakten in Lehrbüchern oder eine Literaturrecherche in Internetforen keine Schande. Fachliches Wissen und ein hohes Maß an Erfahrung, gepaart mit Empathie im täglichen Umgang mit Kolleginnen, Kollegen und mit Patienten erweisen sich als hilfreich für eine erfolgreiche Arbeit an unseren Patienten. Bis dahin ist es ein weiter Weg. Von jüngeren Medizinern erwarte ich insofern, dass sie – unterstützt von erfahrenen Kollegen – im Zuge der Behandlung ihrer Patienten beständig Konzepte und Algorithmen entwickeln, die es ihnen ermöglichen, zielgerichtet in kürzester Zeit die Diagnose eines Patienten zu sichern und ihn anschließend einer erfolgreichen Behandlung zu unterziehen. Damit erfüllen sie ihre Kernkompetenz.

Datenschutz im Wartezimmer und am Empfangstresen. Wo liegen da die Probleme?

Viele Menschen neigen in vielerlei Hinsicht zu extrovertiertem Verhalten und geben beispielsweise in sozialen Netzwerken auch bereitwillig Informationen über sich preis. Dies geschieht meist unter dem Vorwand, man habe soweit alles unter Kontrolle. In Bezug auf ihre Gesundheit scheinen die gleichen Menschen nicht unbedingt zurückhaltender, allenfalls nachdenklicher zu sein. Andere möchten hinsichtlich ihrer Gesundheit grundsätzlich keine Informationen preisgeben. Unabhängig vom individuellen Verhalten der Menschen bewegen wir uns alle interaktiv in einem öffentlichen Raum, in dem von Rechts wegen Datenschutzrichtlinien existieren, die eingehalten werden müssen. Auch die Arztpraxis ist ein solch öffentlicher Raum.

Aus Sicht des Datenschutzes besteht das grundlegende Problem sowohl im Wartezimmer, als auch am Empfangstresen einer Praxis darin, dass wartende Patienten für sie nicht bestimmte Informationen zu anderen Patienten aufschnappen könnten. Dies gilt es zu vermeiden. Auch wenn Patienten mit Informationen zum Gesundheitszustand anderer Patienten an sich nichts anfangen können, ist es vielen unangenehm, wenn Details über ihren Gesundheitszustand öffentlich werden. Leider lassen die baulichen Voraussetzungen der meisten Praxen die Einhaltung von Datenschutzrichtlinien nur bedingt zu. Dennoch darf unterstellt werden, dass die Praxisteams im Rahmen ihrer Möglichkeiten redlich um die Einhaltung des Datenschutzes bzw. um die Wahrung der Privatsphäre der Patienten bemüht sind. Das Einhalten von Abständen zueinander, Sichtschutzmaßnahmen oder das Vermeiden einer zu lauten Kommunikation sind nur einige sinnvolle Maßnahmen. Andererseits darf auch nicht unerwähnt bleiben, dass auch die Patienten sich darauf eingestellt haben, in der Praxis rücksichtsvoll und diskret miteinander umzugehen.

Die Gespräche des Arztes oder der Ärztin mit dem Patienten über seine Krankengeschichte und über seine aktuellen Beschwerden finden natürlich datenschutzgerecht unter Ausschluss der Öffentlichkeit statt.

Jetzt geht es um Datenschutz im Mehrbettzimmer zum Beispiel bei Visiten. Wie sieht es da aus?

In den meisten Krankenhäusern werden überwiegend Zweibettzimmer vorgehalten. In der Regel hat jede Station eines Krankenhauses – auch eines modernen Krankenhauses – zumindest ein Zimmer, in dem bis zu vier Patienten aufgenommen werden könnten.

Wenn in solchen Zimmern Visiten durchgeführt werden, stößt man hinsichtlich des Datenschutzes zwangsläufig auf Grenzen, zumal die Krankengeschichte eines jeden einzelnen Patienten zwischen Arzt und Patienten besprochen wird, zumeist in einer Lautstärke, die das Mithören durch andere Patienten ermöglicht. Angehörige und Freunde, die Patienten besuchen, werden anlässlich der Visiten in der Regel gebeten, das Patientenzimmer zu verlassen. Bei den Visiten geht es in erster Linie darum, mit dem Patienten abzuklären, welche Untersuchungen anstehen, welche Diagnose gestellt worden ist oder welche therapeutischen Maßnahmen durchgeführt werden sollen. Arzt und Patient sollen sich dadurch gegenseitig auf dem Laufenden halten. Während der Visiten könnten aber auch bittere Wahrheiten und Befunde zur Sprache kommen, die nicht für alle im Raum anwesenden Personen bestimmt

sind. Es liegt im Ermessen des visitierenden Arztes, bestimmte Befunde nach Möglichkeit in einem separaten Einzelgespräch sensibel und einfühlsam vorzubringen.

Trotz des Bemühens um Diskretion und trotz der Wahrung der Privatsphäre der Patienten darf eines nicht außer acht gelassen werden: Ein Mehrbettzimmer ist ein öffentlicher kommunikativer Raum. Innerhalb eines Mehrbettzimmers entwickelt sich eine gewisse Solidarität unter den Patienten. Man hat die gleichen Sorgen und Probleme wie der Bettnachbar und das gleiche Ziel, wieder gesund zu werden. Diese Patienten tauschen sich über ihre Krankheiten und Krankheitsverläufe selber aus, so dass innerhalb kurzer Zeit ohnehin alle genau wissen, was der andere Patient hat. Ein gesteigertes Interesse am Datenschutz liegt in diesem Zusammenhang nicht vor. Wer selbst einmal in einem Mehrbettzimmer als Patient gelegen hat, wird dies bestätigen können.

Wie ist der Schutz der Patientenakten gewährleistet – hier mal der altmodischen in Papierform?

Wir befinden uns im Zeitalter des digitalen Umbruchs. Alle Bemühungen laufen darauf hinaus, sämtliche Patientenrelevanten Befunde, Anforderungen, Arztbriefe oder Röntgendarstellungen möglichst vollständig in digitaler Form zu erfassen. Man erreicht diese digitalen Akten nur noch über die an das Netzwerk des Klinikums angeschlossenen Rechner mit Hilfe individueller personenbezogener Passwörter und nur das Fachpersonal der Klinik ist in der Lage, Befunde oder sonstige Schriftstücke zu ergänzen oder Informationen abzurufen. Die digitalen Dokumente sind für die Öffentlichkeit und damit für Unbefugte nicht zugänglich. Dies ist ein wichtiger Schritt zur Sicherung der Patientendaten.

Parallel dazu gibt es auch eine Patientenakte in Papierform. Hier werden in erster Linie Dokumente wie Aufklärungs- und Einwilligungsbögen mit den Originalunterschriften der Patienten und der aufklärenden Ärzte hinterlegt. Auch originale EKG-Ableitungen werden in Papierform dokumentiert und anschließend in der Krankenakte abgelegt. Da Untersuchungsbefunde nahezu ausschließlich digital aufgearbeitet werden, werden sie üblicherweise nicht in der „klassischen" Patientenakte archiviert.

Da die Befunde in der „Papierakte" nicht wie die digitalen Befunde gesichert werden können, müssen die Akten aus Gründen des Datenschutzes für Unbefugte unzugänglich sein, weshalb sie im sog. Stationszimmer unter Verschluss gehalten werden.

Datenschutz-Schwächen wegen Überlastung? „Jetzt auch noch Daten zu schützen, schaffen wir einfach nicht."

Dass der Datenschutz unter der generellen Arbeitsüberlastung auch mal verletzt werden könnte, kann ich nicht sicher ausschließen. Den Schutz unserer Patientendaten im eigentlichen Sinne praktizieren wir ja bewusst und unbewusst jeden Tag, unabhängig von der Arbeitsbelastung. Es ist auch nicht so, dass wir jeden Tag daran denken oder darauf hingewiesen werden müssen, besonders datenschutzkonform zu arbeiten, weil dies eigentlich zu einer Selbstverständlichkeit geworden ist. Das Schützen der Daten erfordert bei gut administrierten Computersystemen auch keine zusätzliche Arbeit. Ich will das an einem Beispiel erklären: Wenn ich einen für alle Mitarbeiter zugänglichen Rechner auf einer Station benutze und meine Arbeit an einer Patientendatei beendet habe, dann schließe ich meinen Account wieder so ab, dass nur die legitimierten Kolleginnen und Kollegen mit ihrem eigenen Passwort Zugriff auf die entsprechenden Dateien haben, die ich neu in die Patientenakte aufgenommen habe. Für andere ist der Zugriff gesperrt.

Zusätzliche Arbeit wird beispielsweise dadurch hervorgerufen, dass im Rahmen der medizinischen Behandlung jeder Handgriff des Arztes und auch der Pflegekraft dokumentiert werden muss. Die Krankenversicherungen wollen nur dann entsprechende Erlöse zahlen, wenn auch medizinische Maßnahmen wie z. B. das Anlegen einer Kanüle oder Physiotherapie, das Durchführen von Beatmungstechniken genau dokumentiert wird. Mit solchen Auflagen haben wir bei der Einhaltung des Datenschutzes nicht zu kämpfen.

Behinderung der Behandlung durch Datenschutz-Hürden? Z. B. fehlende Erlaubnis der Datenübertragung zwischen den diversen Abteilungen und zwischen den medizinischen Abteilungen und den oftmals ausgegliederten Service-Unternehmen (Catering, Transporte und Logistik ...)

Die Wahrscheinlichkeit, im Zuge der allgemeinen Behandlung von Patienten innerhalb einer Klinik auf Datenschutzhürden zu treffen, die sich nachteilig auswirken könnten, ist eher gering. Im Interesse einer sachgerechten Behandlung unserer Patienten sind die Handlungsspielräume und Datenflüsse von Rechts wegen bewusst großzügig ausgelegt worden, sowohl im Hinblick auf die Zusammenarbeit verschiedener Berufsgruppen, als auch im Hinblick auf die Inanspruchnahme verschiedener Fachabteilungen innerhalb und außerhalb der Klinik. Auf dieser Grundlage findet die Kommunikation bzw. der Datenaustausch zwischen den verschiedenen Fachabteilungen einer Klinik mit immensen Datenflüssen statt, aber auch die klinikübergreifende Kommunikation im Zuge einer notwendigen externen Verlegung von Patienten in eine andere Fachklinik unter Einbeziehung des Rettungsdienstes. Auch Serviceunternehmen, die notwendige Dienstleistungen wie Catering, Reinigung, Transport oder Logistik erfüllen, sind in die Klinikabläufe integriert. Diese verfügen in der Regel über keine Befugnisse hinsichtlich der medizinischen Patientendaten.

Grundsätzlich sind alle Mitarbeiterinnen und Mitarbeiter, die in medizinischen Einrichtungen tätig sind, unabhängig davon, ob regelmäßiger Patientenkontakt besteht oder nicht, zur Verschwiegenheit verpflichtet und dürfen ihre persönlichen Eindrücke streng genommen im privaten Bereich nicht kommunizieren.

Sofern in speziellen Situationen dennoch Bedenken hinsichtlich der Einhaltung des Datenschutzes oder Zweifel hinsichtlich der Legitimation bestimmter Maßnahmen bestehen, bedarf es individueller Lösungen. Sofern die Klinik über einen Datenschutzbeauftragten

verfügt, können strittige Fragen zum Datenschutz zeitnah geklärt werden.

Haben Sie abschließende Bemerkungen?

Es gibt durchaus Situationen, in denen sich Mitarbeiter aus medizinischen Bereichen beispielsweise auf der Bus- oder Bahnfahrt nach Hause trotz ihrer Verpflichtung zur Verschwiegenheit über bestimmte Behandlungsfälle unterhalten. Ob gewollt oder nicht werden andere Fahrgäste genötigt, solchen Gesprächen zuzuhören. Dabei werden Informationen und Abläufe innerhalb der Klinik oder Praxis mit oft negativer Färbung wiedergegeben, die auch die Behandlung von Patienten einschließt. Auch wenn keine Namen genannt werden, so werden Situationen häufig so geschildert, dass unter Umständen Rückschlüsse auf die betroffenen Personen möglich wären.

Ein weiteres Problem möchte ich abschließend noch erwähnen: Viele Besucher finden es so „cool", wenn sie trotz Fotografierverbot im Krankenhaus Selfies aufnehmen und diese dann unter Missachtung der Privatsphäre anderer Menschen in den sozialen Netzwerken verbreiten. Im Hinblick auf die Technologien der automatisierten Gesichtserkennung im Internet sehe ich da sehr große Probleme.

Auf der einen Seite werden wir als in der Klinik Tätige ermahnt, den Datenschutz jederzeit zu wahren. Wenn auf der anderen Seite Besucher oder gar Patienten selbst den Datenschutz verletzen, sind wir leider oft machtlos und unsere Bemühungen sind vergebens.

* Der Interviewpartner ist der Redaktion namentlich bekannt. Die Genehmigung zur Autorennennung konnte durch die Klinik wegen der Coronavirus-Krise vor dem Druck nicht rechtzeitig erteilt werden.

Heinz Alenfelder

Nach dem Essen sollst du ruh'n, oder ... 1000 Schritte zur alltäglichen Überwachung

Am Anfang war es vielleicht der Body-maß-Index oder ein Schrittzähler, dann die spezielle Trainings-App des Fitness-Clubs oder die Kalorien-Überwachung im Diät-Programm, und heute? Die weltgrößte Suchmaschine wirft beim Stichwort „Gesundheits-App" etwa 12 Millionen Ergebnis-Treffer aus und allein im Google-Play-Store finden sich über 100.000 Apps aus dem Bereich Health/ Fitness[1]. Das Thema Gesundheit ist in aller Munde und bald wohl auch auf aller Smartphone. Eigentlich könnte es uns damit viel besser gehen. Doch wie sieht es mit den erfassten Daten aus? Der Bundesgesundheitsminister ist der Meinung „Datenschutz ist was für Gesunde"[2] und er fordert ein „weniger verkrampftes Verhältnis zum Umgang mit den Daten"[3]. Warum der Datenschutz bei allen Apps im Argen liegt, insbesondere bei denjenigen, die Vitaldaten erheben, soll im Folgenden aufgezeigt werden. Dazu stellt der Artikel mit einigen Studien der letzten Jahre zunächst die aktuelle Praxis der Datenübermittlung vor allem durch Fitness- und Gesundheits-Apps dar. Dann wird der Blick auf die diesbezügliche Kontrolle durch Datenschutz-Aufsichtsbehörden gerichtet um abschließend Hinweise für die App-Entwicklung zu geben.

Generell ist allgemein bekannt und unumstritten, dass sehr viele Apps Daten erheben und an Hersteller oder an Apple oder Google übermitteln. So berichteten wir in der DANA 3/2019[4] von einem App-Betreiber der spanischen Fußball-Liga. Diesem wurde seitens der Aufsichtsbehörde ein Bußgeld auferlegt, weil die App ungefragt das Smartphone-Mikrofon nutzte, um zusammen mit Positionsdaten des mobilen Geräts während der Sendezeit der Liga zu analysieren, ob die jeweilige Gaststätte auch Lizenzgebühren bezahlte. Ebenso offenbarte eine im Frühjahr 2018 veröffentlichte Tracking-Studie der Universität Oxford umfassende Überwachung[5]: Nur 10 % der geprüften Apps erfassten keine Daten, fast 90 % sendeten Daten an Google. Big-Data-Algorithmen erlauben dem Großkonzern heute, mit diesen Daten Einstellungen, Vorlieben und zukünftige Verhaltensweisen der Nutzenden zu berechnen; bereits vor zwanzig Jahren wurde in einer amerikanischen Studie gezeigt, dass allein Geburtsdatum, Postleitzahl und Geschlecht ausreichen, um 80 % der Bevölkerung zu identifizieren[6].

Studien zu Fitness- und Gesundheits-Apps

Angesichts der weiten Verbreitung von Fitness-Apps (im englisch-sprachigen Raum auch als „self-tracking" vor allem der „quantified self"[7]-Bewegung bezeichnet), die personenbezogene Daten in allen Lebenslagen erfassen, hat ein Forschungsteam der **Open University** um Luke Hutton ein Verfahren entwickelt, mit dem herauszufinden ist, wie Apps sich in Bezug auf die Privatsphäre verhalten[8]. Interessant sind die durchaus praktischen Fragestellungen, die zu insgesamt 26 heuristischen Kriterien führten. So sollten sich App-Nutzende die folgenden Fragen stellen:

1. Werde ich vor dem Start der App darüber informiert, was mit meinen Daten geschieht?
2. Habe ich die Kontrolle über meine Daten, wenn ich die App benutze?
3. Kann ich auf die von mir erzeugten Daten zugreifen?
4. Habe ich die Möglichkeit, die Weitergabe von Daten an Dritte zu unterbinden?

Bei den 64 getesteten Android-Apps, so fanden die Forscher heraus, erfüllte die Mehrheit nicht die entwickelten Kriterien, die sowohl die Information der Nutzenden über Datenübermittlung als auch den Einblick in die Daten selbst umfassen. Im Gegenteil: nur eine einzige App (Timesheet) überzeugte, indem sie allen Kriterien gerecht wurde. Diese App speichert die Daten lediglich lokal auf dem Smartphone. Der Durchschnitt aller Apps erreichte nicht einmal die Hälfte der Skala. Insgesamt konnte aber nicht von der Kategorie der App auf die Erfüllung von Datenschutz-Kriterien geschlossen werden, wenn auch allgemein festgestellt wurde: *„Weight-tracking apps performed best, and cycling apps performed worst“*[9]. Besonders bedenklich scheint dem Forschungsteam die Tatsache, dass die Fitness-Apps weniger problematisch im Umgang mit dem Datenschutz waren, als die Gesundheits-Apps (mHealth-Apps). Sie führen das auf das wirtschaftliche Interesse an den gewonnenen sensiblen Daten zurück (*„significant commercial value“*).

In Australien veröffentlichten Huckvale und andere eine Untersuchung aus dem Jahr 2018 über 36 erstplatzierte **Depressions- und Raucher-Entwöhnungs-Apps**[10]. Sie hatten vorab festgestellt, dass bei Demenz-Unterstützungs-Apps nur in 4 % der Fälle schriftlich zugesichert worden war, Nutzungsdaten würden nicht verkauft; bei Diabetes-Apps waren es immerhin 22 %. In ihrer Analyse wollten sie herausfinden, inwieweit solche Erklärungen auch den tatsächlichen Datenübertragungen der Apps entsprechen. Zwei Drittel der geprüften Apps hatten zumindest einen Link zur Datenschutzerklärung. In etwa der Hälfte gab es Hinweise zum Opt-Out und Löschen vorhandener Daten. Während nur eine einzige App explizit ausschloss, Daten mit Dritten zu teilen, übermittelte fast die Hälfte der Apps Daten, ohne darauf hinzuweisen – wenn überhaupt eine Datenschutzerklärung vorlag. Drei Apps übermittelten sogar Daten, obwohl sie explizit diese Übertragung ausgeschlossen hatten. Und obwohl Google und Facebook von den Entwicklern verlangen, dass auf die Nutzung ihrer Dienste in den Erklärungen hingewiesen werden muss, erfolgte das bei nahezu 50 % der Apps nicht! Das deckt sich im übrigen mit verschiedenen Veröffentlichungen[11], die darauf hinweisen, dass Apps wie Flo, HRMonitor oder Realtor ungefragt sensitive Gesundheitsdaten zwecks Werbung an Facebook weitergeben, selbst dann, wenn der oder die Betroffene kein Facebook-Konto besitzt.

Ein Forschungsteam der Universitäten Sydney, Toronto und Kalifornien um Quinn Grundy nahm in ähnlicher Weise 24 bestplatzierte **Apps mit Medizin-Bezug** unter die Lupe[12]. 79 % der untersuchten Apps übermittelten Daten wie den Geräte-Namen, die Betriebssystem-Version oder auch die E-Mail-Adresse an Entwickler oder Dritte. Ein Drittel der Apps nutzten Web-/Cloud-Dienste für App-Analyse oder Werbung und bei zwei Dritteln vermuten die Forscher, dass durch die Datensammlung und -analyse ein erhöhtes Sicherheitsrisiko besteht. Hinzu kommt, dass die Mehrheit der Firmen, die als Dritte (third party) die Daten übermittelt bekommen, einräumt, ihrerseits die Daten wieder weiterzugeben (fourth parties). Bei all diesen Datenübermittlungen fehlt den Nutzenden der Apps jegliche Transparenz, ganz zu schweigen von der Kontrolle: *„users do not own or control their personal data“* und die Forscher fordern entsprechend, dass einerseits die Ärzte Patienten auf die Gefahren hinweisen müssten und andererseits die Entwickler über alle Datenübertragungen informieren und eine Einstellmöglichkeit bieten sollten.

Datenübermittlung durch Apps und Datenschutzerklärungen

Auch eine **Studie von Tech Crunch** lenkt den Blick gezielt auf Third-Party-Software. Im Februar 2019 berichtete Nancy Lindsey[13] über diese Studie, die Sitzungsprotokollübermittlung bei Buchungen per Expedia, Air Canada oder Hotels.com feststellte. Deren iPhone-Apps nutzen die „session replay“-Technologie, mit der Entwicklungsfirmen feststellen können, welche Probleme bei Nutzung der App auftreten. Dabei werden Screenshots (digitale Fotos von Bildschirm-Inhalten) beim Benutzen der App auch ohne Einverständnis der Nutzenden an die App-Entwickler-Firmen gesendet, ohne darin enthaltene personenbezogene Daten unkenntlich zu machen. Lindsey erwähnt in diesem Zusammenhang Ausweis- und Kreditkarten-Nummern. Unmittelbar nach Veröffentlichung der Studie hat Apple seine Entwickler darüber informiert, dass das Sammeln persönlicher Daten per „session replay“- und Tracking-Technologie den „App Store Review Guidelines“ widerspreche und dass entsprechend agierende Apps aus dem App-Store entfernt werden würden. Die Firma Glassbox sowie andere Firmen, die Software für die „session replay“-Technologie entwickeln, betonten laut Bericht, dass dies keine Spionage-Software sei. Glassbox äußerte: *„The technology was not intended for spying purposes“*. Chris Olson, CEO von The Media Trust, fordert App-Entwickler auf, genauer zu hinterfragen, was die Software solcher Third-Party-Anbieter eigentlich tut. Sie sollten nicht nur über die eigene Datenverarbeitung, sondern auch über die der genutzten Zusatzsoftware in den Privacy Policies informieren. Olson kommt zur Einschätzung, dass *„This widespread blind spot toward third party code can cost companies their reputation“*.

Das Thema der **Screenshot-Übermittlung** gelangte übrigens bereits 2017 bezüglich einer App des Fahrtvermittlers Uber in die Schlagzeilen[14]. Damals ging der Sicherheitsforscher Will Strafach allerdings davon aus, dass die Uber-App die einzige App war, die von Apple die Berechtigung zur Aufzeichnung von Screenshots im Hintergrund erhalten hatte.

Ebenso hat eine **Studie aus Norwegen**[15] das Verhalten von 21 beliebten kostenfreien Android-Apps analysiert. Innerhalb von zwei Analyse-Tagen wurden durch 19 Apps Daten an insgesamt 600 Empfänger übermittelt, von denen die meisten in den USA beheimatet sind. In einigen Datenschutzerklärungen wurde auf diesen Tatbestand nicht hingewiesen; bei drei der Apps fand die Übermittlung trotz gegenteiliger Versicherung in der Datenschutzerklärung statt.

Nicht nur angesichts solcher Ergebnisse ist es unabdingbar, dass vor der Installation einer App auf einem Smartphone auf Datenübermittlungen hingewiesen wird. In dieser Hinsicht gibt die Studie des Bundesministeriums für Justiz und Verbraucherschutz **„Verbrau-**

cherinformationen bei Apps – Empirie"[16] allerdings Anlass zu ernsthafter Besorgnis. Laut Abschlussbericht der von Infas durchgeführten Studie bildet die „empirische Bestandsaufnahme" zu Informationen und Datenschutz bei Apps *„die wissenschaftliche Basis für die verbraucherpolitische Arbeit des BMJV"*. Konkret wurden im Jahr 2017 insgesamt 200 relevante Apps auch bezüglich der Datenschutzfreundlichkeit überprüft. Dabei standen im Vordergrund

- die Erläuterung zur Funktionsweise der App im Vorfeld des Downloads,
- die Bereitstellung aller relevanten Informationen im Zusammenhang mit der Nutzung der App, sowohl im Vorfeld als auch während der Nutzung,
- die Vollständigkeit und Datenschutzfreundlichkeit der Datenschutzerklärung,
- die Notwendigkeit der eingeforderten Zugriffsberechtigungen für die Funktionalität der App,
- die Individualisierbarkeit der Datenschutzeinstellungen (z. B. durch Opt-In- bzw. Opt-Out Möglichkeiten) sowie
- das Datensendeverhalten der App.

Es stellte sich heraus, dass sowohl Quantität als auch Qualität der meisten, oft sehr langen Datenschutzerklärungen mangelhaft sind. Da diese auch oft nicht in der App zur Verfügung stehen, empfiehlt das Forschungsteam, die Hinweise direkt im App-Store zu platzieren, sie inhaltlich konkret auf die App-Nutzung zu beziehen und außerdem auf gut 1000 Wörter zu kürzen. Erstaunlich ist auch, dass besonders in den Bereichen Spiele, Kinder und Fitness/Gesundheit *„deutliche Defizite bei der Verfügbarkeit der Datenschutzerklärung festgestellt"* wurden. Die Mehrheit der Apps schneidet schlecht ab, keine App erreichte die Bestnote, nur 4 % erreichten ein „gut". Außerdem wurde geprüft, ob beim ersten Öffnen aktiv auf die Datenschutzbestimmungen hingewiesen wird. Das war bei 70 % der Fitness-/Gesundheits-Apps nicht der Fall.

Forderungen der Datenschutz-Aufsichtsbehörden

Bereits 2012 gab die **Kanadische Datenschutz-Aufsichtsbehörde** einen Leitfaden für die App-Entwicklung[17] heraus. In der darin enthaltenen Checkliste wird die Verantwortung der App-Entwickler für die Datenverarbeitung hervorgehoben und ein besonderer Schwerpunkt auf Transparenz gelegt: *„Be open and transparent about your privacy practices"*. Gemäß dieser Forderung soll die Datenschutzerklärung (privacy policy) den Nutzenden in einfacher Sprache erklären, was die App mit den erhobenen Information tut. Um das auf den kleinen Bildschirmen der Mobilgeräte optimal zu gestalten, empfiehlt die Checkliste, verschiedene Ebenen zu nutzen, eine Übersicht über die Datenschutzeinstellungen mit Änderungsmöglichkeit anzubieten und visuelle Elemente wie Grafiken, Farben und Töne einzusetzen. Schließlich wird betont, dass die Datensammlung nicht über das Benötigte hinausgehen soll: *„Do not collect data because you think it may be useful in the future"*.

Ein Jahr später, 2013, erschien das Papier „Opinion 02/2013 on apps on smart devices"[18] der europäischen **Article 29 Data Protection Working Party**, in dem die Problematik ausführlich geschildert wird und verschiedene konkrete Anweisungen und Empfehlungen an App-Entwickler, Geräte- und Betriebssystem-Hersteller, App-Stores und Third-Party-Entwickler gegeben werden. Darunter befindet sich auch eine 14-Punkte-Liste, in der beispielsweise zum automatischen Löschen des Accounts bei Inaktivität aufgerufen wird: *„App developer must […] predefine a period of inactivity after which the account will be treated as expired"*.

Der **Düsseldorfer Kreis** (der deutschen Datenschutzaufsichtsbehörden im nichtöffentlichen Bereich) veröffentlichte 2014 die „Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter"[19]. Laut Eigenaussage zeigt sie *„datenschutzrechtliche und technische Anforderungen auf und macht diese anhand plakativer Beispiele verständlich"*. 2016 hat das Bayerische Landesamt für Datenschutzaufsicht einen darauf aufbauenden, 45 Punkte umfassenden „Prüfkatalog für den technischen Datenschutz bei Apps mit normalem Schutzbedarf"[20] erstellt. Auf dessen Basis finden augenscheinlich die Kontrollen durch die Aufsichtsbehörde statt. Da sich die Orientierungshilfe am damaligen Gesetzesstand abarbeitet, ist sie heute unter der DSGVO nur bedingt nutzbar, besteht doch bei allen Verweisen Unsicherheit über die aktuelle Rechtslage.

Im Bezug auf das Vorgehen bei der Überprüfung, ob eine App die gesetzlichen Bedingungen einhält, beschloss die **Datenschutzkonferenz** (der Bundes- und Landesdatenschutzbeauftragten) in ihrer „Hambacher Erklärung"[21] im Frühjahr 2019 anlässlich der Übertragung von Daten an Facebook (automatisch bei Nutzung des Software-Development Kits) *„Prüfszenarien für eine entsprechende Kontrolle von Apps zu entwickeln"*, deren Ziele gemeinsame Prüfstrategien und Kontrollen sind.

Hinweise für die App-Entwicklung

Bei der Suche nach möglichst konkreten Hinweisen für die App-Entwicklung sticht auf europäischer Ebene der **„Privacy Code of Conduct on mobile health apps"**[22] des European Data Protection Board hervor. Die Arbeit an diesem Verhaltenskodex wurde 2015 aufgenommen und kurz vor dem Inkrafttreten der EU-Datenschutz-Grundverordnung (DSGVO) fertig gestellt. Die Anpassung an die DSGVO steht noch aus, doch sollten auch jetzt schon die Hinweise bei der App-Entwicklung beachtet werden. Sie beinhalten unter anderem Forderungen bezüglich

- Einverständniserklärung (user consent) – frei, spezifisch und informiert
- Zweckbindung und Datenminimierung (purpose limitation and data minimisation) – Verarbeitung nur für spezifische und legitimierte Zwecke; Verarbeitung nur der absolut notwendigen Daten
- Privacy by Design und by Default – Beachtung des Datenschutzes in jedem Entwicklungsschritt und bei jeder Wahlmöglichkeit für den Nutzenden; defaultmäßig datensparsame Voreinstellungen
- Werbung (advertising) – Unterscheidung zwischen Werbung, die auf personenbezogenen Daten basiert (Opt-In-Einverständniserklärung zwingend) und allgemeiner Werbung (Opt-Out möglich)
- Übermittlung an Dritte (disclosing data to third parties for processing

operations) – Vorabinformation des Nutzenden; bindender Vertrag mit dem/der Dritten.

Weitere, teils ausführliche Hinweise sowohl für die Entwicklung als auch für die Benutzung von Gesundheits-Apps finden sich in der aus den Jahren 2015/2016 stammenden umfassenden Studie **„Charismha“**[23] der **Medizinischen Hochschule Hannover**, die durch das Bundesgesundheitsministerium gefördert wurde. Allerdings sind die Hinweise an die Entwickler naturgemäß allgemeiner Natur, so dass zu fragen ist, wie in einem konkreten Fall vorgegangen werden soll. Dies stellte Corinna Giebler mit ihrer Arbeit an der Universität Stuttgart 2017[24] anhand des Gesundheitsspiels **„Secure Candy Castle“** vor, in das sie exemplarisch Datenschutzmechanismen einbaute. Durch die Verbindung des Spiels mit einem Datenschutzsystem ist es bei der Benutzung möglich, selbst zu entscheiden, welche sensiblen Daten mit der App geteilt werden sollen. Der interessante Aspekt dieser Arbeit ist die Anpassung der App-Funktion an die individuell getroffenen Einstellungen. Dies war bis dato in anderen Gesundheits-Apps nicht realisiert.

Das oben erwähnte Team von **Hutton an der Open University** sieht seine Evaluations-Methode als Möglichkeit für Entwickelnde, den Grundsatz Privacy by Design umzusetzen: *„Our heuristic evaluation method supports the retrospective evaluation of privacy in self-tracking apps and can be used as a prescriptive framework to achieve privacy-by-design in future apps.“*[25]

Insgesamt aber, so stellt **Trix Mulder von der Universität Groningen** fest[26], ist die Diskrepanz zwischen den Marketing-Aussagen zu Gesundheits-Apps und den Datenschutzerklärungen sehr groß und kann nur dadurch behoben werden, dass App-Entwickler aus dem Gesundheitsbereich mit den nationalen und europäischen Datenschutzaufsichtsbehörden ähnlich intensiv zusammenarbeiten wie dies der Gesundheitssektor mit der pharmazeutischen Industrie bereits praktiziert: *„together they can create solutions which benefit all“*. Allerdings stellt sie auch klar, dass Gesetze und Kontrolle allein nicht reichen, sondern Kampagnen verschiedener gesellschaftlicher Gruppierungen das Thema voran bringen müssen: *„It is also very much a societal challenge, which could be addressed by societal organisations (such as patient organisations, consumers associations, etc.) via various campaigns.“*[27] Dies kann aus Sicht der DVD nur unterstützt werden.

1 https://42matters.com/stats

2 https://www.deutsche-apotheker-zeitung.de/news/artikel/2016/09/13/jens-spahn-philosophiert-ueber-die-zukunft-der-versorgung

3 DANA 2/2018, 103

4 DANA 3/2019, 162

5 DANA 1/2019, 49

6 https://dataprivacylab.org/projects/identifiability/paper1.pdf

7 https://de.wikipedia.org/wiki/Quantified_Self

8 https://mhealth.jmir.org/2018/10/e185/

9 siehe Endnote 8, S. 6 https://mhealth.jmir.org/2018/10/e185/

10 https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2730782

11 DANA 2/2019, 103

12 https://www.bmj.com/content/bmj/364/bmj.l920.full.pdf

13 https://www.cpomagazine.com/data-privacy/many-popular-iphone-apps-are-recording-screens-without-user-privacy-consent/

14 DANA 4/2017, 218

15 https://journals.sagepub.com/doi/abs/10.1177/0894439318777706

16 https://www.bmjv.de/SharedDocs/Downloads/DE/Service/Studien UntersuchungenFachbuecher/Verbraucherinfos_Apps.html

17 http://www.priv.gc.ca/information/pub/gd_app_201210_e.pdf

18 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

19 https://www.lda.bayern.de/media/oh_apps.pdf

20 https://www.lda.bayern.de/media/baylda_pruefkatalog_apps.pdf

21 https://www.datenschutzkonferenz-online.de/media/pr/20190403_pr_hambacher_schloss.pdf

22 https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps

23 https://charismha.weebly.com/uploads/7/4/0/7/7407163/charismha_gesamt_v.01.3-20160424.pdf

24 B. Mitschang et al. (Hrsg.): BTW 2017 – Workshopband, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017, S. 311-320

25 siehe Endnote 8: https://mhealth.jmir.org/2018/10/e185/

26 http://ejlt.org/article/view/667/898

27 https://www.tandfonline.com/doi/pdf/10.1080/13600834.2019.1644068

Mike Kuketz

Implantateregister-Errichtungsgesetz „Zu Risiken und Nebenwirkungen fragen Sie den Gesundheitsminister“

1 Bittere Medizin

Man mag hinter dem Titel „Implantateregister-Errichtungsgesetz (EIRD)“[1] zunächst die Spannung eines Beipackzettels vermuten. Was man allerdings zu lesen bekommt, ist eine konzentrierte Dosis „Gesundheits-Big Data“. Überraschen kann dies nicht, sofern man die „Digitalcharta Innovationsplattform: D“ der CDU gelesen hat. Die Partei will dort „weg vom Grundsatz der Datensparsamkeit und hin zur Datensouveränität“.[2]

Stellt man der Datenminimierung diesen Begriff gegenüber, mag man zwar Datensouveränität schreiben, meint aber **Datenreichtum**. Gleichzeitig hat für die CDU die Willensbekundung eines Bürgers in Form einer Einwilligung ausgedient: „Die Regulierung des Datenschutzes basiert zentral darauf, dass Nutzer der Verarbeitung ihrer Daten zustimmen. Was früher ein plausibles Konzept war, funktioniert heute nicht mehr.“[3]

Denn den Imperativ von Big Data hat die CDU augenscheinlich verinnerlicht: **Daten müssen frei fließen**. Auch bei sensiblen Gesundheitsdaten „müssen Daten im Gesundheitssystem – unter Berücksichtigung des Schutzes personenbezogener Daten – erstens frei fließen“.[4]

Wem nun bittere Medizin schwant, liegt (leider) richtig. Denn das EIRD verpflichtet Implantat-Empfänger Gesundheitsdaten in einem **zentralisierten** Register speichern, verarbeiten und „pseudonymisiert“ zur weiteren Nutzung zu überlassen. Die Pflicht zur Datenbereitstellung ersetzt eine informierte Zustimmung des Patienten oder der Patientin und degradiert ihn oder sie zum **zwangsrekrutierten Datenlieferanten** für eine umfangreiche Gesundheitsdatenbank. Zu hart geurteilt? Kaum. Denn, so verrät uns § 16 des Gesetzes, insbesondere Anamnese- und Befunddaten, Voroperationen, sowie Gewicht und Größe gehören zu den meldepflichtigen Daten. Der Datenschatz der im Vertrauensverhältnis zwischen Arzt und Patient auf einem Anamnesebogen[5] weitergeben wird, kann nach dem Big Data Imperativ nicht unter dem Schutzmantel der ärztlichen Schweigepflicht verbleiben.



Bild: iStock

Um es konkret anhand eines Beispiels darzustellen: Es kann viele persönliche und medizinische Gründe haben, warum eine geneigte Leserin Brustimplantate benötigt. Diese Entscheidung mag teilweise selbstbestimmt, aber auch den Umständen geschuldet sein. Aber über die Information(en), ob sie übergewichtig ist, raucht, an Heuschnupfen leidet oder zur Verhütung die „Pille“ verwendet, bestimmt sie fortan nicht mehr. Denn diese Daten mehren nun den Datenreichtum des Gesundheitssystems. Wer sich nun fragt, welche Implantate noch von dem Gesetz umfasst sind:[6]

- Herzklappen / andere kardiale Implantate,
- implantierbare Defibrillatoren,
- Herzschrittmacher,
- Cochlea-Implantate,
- Neurostimulatoren,
- Brustimplantate,
- Gelenkendprothesen,
- Bandscheibenprothesen,
- Wirbelkörperersatzsysteme,
- Stents.

Nebenbei bemerkt: Die Pseudonymisierung soll zwar „eine Identifizierung ausschließen“.[7] Fraglich ist allerdings, wie der Einsatz einer eindeutigen, unveränderbaren ID, wie der Krankenversichertennummer, als Grundlage (§ 9 Abs. 2 EIRD) dazu geeignet ist, den angegebenen Zweck zu erfüllen. Vielmehr scheint ein eindeutiger Identifier vonnöten zu sein, um die anfallenden Daten korrekt zuordnen zu können – die Facebook User-ID lässt grüßen.

2 Gefühl des Ausgeliefertseins

Sofern sich nun ein Gefühl des Ausgeliefertsein beim Leser einstellt und er sich erhofft, zumindest ein Widerspruchsrecht zu haben, der übersieht, dass „Daten frei fließen müssen“. Anomalien, wie eine individuelle Entscheidung sind bei Big Data nicht vorgesehen. Deswegen hat Herr Spahn konsequent den Anspruch auf Widerspruch oder Einschränkung der Verarbeitung (also Sperrung) ausgeschlossen (§ 26

EIRD) – mit der Ausnahme für Daten, die aus bereits bestehenden Registern übernommen werden.

Ein Ausschluss von Betroffenenrechten mag bei Kontaktdaten unter Umständen noch zu rechtfertigen sein, sofern ein Implantat-Typ Probleme verursacht und der Betroffene rasch informiert werden muss. Hier mag die Begründung greifen, dass ein **Allgemeininteresse**[8] gegenüber dem Recht auf informationelle Selbstbestimmung überwiegt. Den Zweck der Kontaktaufnahme suggeriert zwar indirekt der Gesetzestitel. In Wahrheit gehen die erhobenen Daten weit über das erforderliche Maß dieser staatlichen Fürsorge hinaus. Insofern scheint sowohl die Pflicht die Daten bereitzustellen als auch jeden Widerspruch zu unterbinden nur konsistent mit der Digital Charta der CDU. Dies ist auch kein Zufall, denn Herr Spahn wollte so verpflichtend wie möglich, mit so wenig „Ausweichmöglichkeiten" wie nötig, die Datennutzung ermöglichen.[9]

Man liest zwar in der Gesetzesbegründung des EIRD mit Erstaunen, dass ein freiwilliges Register für Endoprothesen der Deutsche Endoprothesenregister (EPRD) mit einer Teilnehmerquote von 90% aufwarten kann[10] – offenbar hat hier das Konzept der Einwilligung funktioniert. Interessanterweise scheinen im Falle des EPRD das eigentliche Problem die Gesundheitseinrichtungen zu sein, die sich nur rund zu 60% beteiligen.

3 Entgegen aller Bedenken

Sei es wie es sei; auch entgegen der Bedenken des Bundesrates (fehlendes Widerspruchrecht)[11] hat der Herr Spahn unbeirrt den freien Fluss der Gesundheitsdaten ermöglicht. Natürlich geht es dem Bundesgesundheitsminister, wie er selbst sagt, nicht darum, die Daten von Max Müller nachzuvollziehen (siehe Video En. 9). Denn das Individuum spielt bei Big Data auch keine Rolle – lediglich der Datenfluss ist entscheidend. Dennoch trägt der Betroffene das volle **unkalkulierbare Risiko**. Erst diesen September hatte Jens Spahn noch den Eindruck, es nehmen immer noch nicht alle, aber immer noch zu viele, das Thema Datensicherheit zu sehr auf die leichte Schulter.[12] Wir erinnern uns, u.a. waren Röntgenaufnahmen frei im Netz zugänglich.[13]

Natürlich sollen die Daten nach dem EIRD Schutzmaßnahmen unterliegen – Datensicherheit, nur Einsicht durch Personal mit Schweigepflicht, Pseudonymisierung, Anonymisierung, verschlüsselte Übertragung. Diese Faktoren spielen allerdings nur nachgeordnet eine Rolle, denn die schiere Breite (Volume) und Tiefe (Variety) der erhobenen Daten ermöglicht jederzeit jedem Empfänger eine **Re-Identifizierung**. Die unkontrollierte Weitergabe innerhalb des Big-Data-Datenflusses an einen großen Empfängerkreis (Hochschulen, öffentliche Stellen, andere Einrichtungen die wissenschaftliche Forschung betreiben, verantwortliche Gesundheitseinrichtungen, medizinische Fachgesellschaften) zu „wissenschaftlichen Zwecken" (§1 Abs. 2 Nr. 6 EIRD) ist das erste Kernproblem. Denn es führt zu einer, diesem Konzept inhärent anhaftenden **Intransparenz**. Weder der Betroffene, noch einer der Verantwortlichen ist in der Lage, Verstöße gegen die Datensicherheit zu bemerken, geschweige denn aufzuklären oder Abhilfe zu schaffen. Datensätze unterliegen genauso wenig wie Algorithmen einer ärztlichen Schweigepflicht. Letztlich ist zudem **ungewiss**, ob die wissenschaftlichen Ergebnisse dann auch dem Allgemeinwohl dienen werden oder der neoliberalen Risikominimierung des Faktors Mensch zuarbeiten – dessen vorgeblich irrationales Verhalten vorhergesagt und eingehegt werden muss, um alle gesellschaftlichen Prozesse möglichst effizient und wirtschaftlich zu gestalten.

4 Fazit

Wie der Report „Special Rapporteur on extreme poverty and human rights" der UN in der Zusammenfassung sagt: „The digital welfare state is either already a reality or is emerging in many countries across the globe. [...], systems of social protection and assistance are increasingly driven by digital data and technologies that are used to automate, predict, identify, surveil, detect, target and punish."[14] „Der Mensch steht im Mittelpunkt". So steht es mehrfach in der Digital Charta der CDU. Bei Big Data stehen die Daten eines Menschen im Mittelpunkt.

Denjenigen, denen es an Ausgewogenheit in diesem Kommentar fehlt, durch die abwesende Aufzählung der Vorteile und Chancen, die aus diesem Gesetz entstehen, möchte ich folgendes entgegnen: „The justification is simple. There are great many cheerleaders extolling the benefits, but all too few counselling sober reflection on the downsides."[15] Das kritische Hinterfragen wäre wohl auch die Aufgabe des Bundesdatenschutzbeauftragten Ulrich Kelber gewesen. Nur findet sich sein Name nicht auf der Tagesordnung der öffentlichen Anhörung vom Juni 2019. Es stellt sich die Frage, ob er überhaupt eingeladen war.

Der oben stehende Text wurde erstmals veröffentlicht unter www.kuketz-blog.de.

1 Implantateregister-Errichtungsgesetz – EIRD, v. 12.12.2019, BGBl. I S. 2494.

2 CDU-Digitalcharta, https://www.cdu.de/system/tdf/media/dokumente/2019-09-30-digitalcharta-antragsfassung-mit-zeilennumerierung.pdf?file=1&type=field_collection_item&id=19580, Seite 3 Rn 96.

3 CDU-Digitalcharta (En. 2), Seite 43 Rn. 643.

4 CDU-Digitalcharta (En. 2), Seite 16 Rn. 557.

5 Siehe dazu ein Beispiel unter https://www.dr-foeste.de/media/shop/layout/home/foeste-anamnese.pdf.

6 Anlage zu § 2 Nr. 1, BGBl. I 2019, 2505.

7 Gesetzesbegründung, BReg, BT-Drs. 19/10523 v. 29.05.2019, S. 80 zu § 9 zu Absatz 3.

8 BT-Drs. 19/10523, S. 37.

9 Mehr Tempo für die Digitalisierung: Jens Spahn auf der DMEA 2019, https://invidio.us/watch?v=p3zwGRQ4ilQ (Video).

10 BT-Drs. 19/10523, S. 39.

11 BT-Drs. 19/10523, S. 112.

12 Patienten-Datenleck: Spahn appelliert an Gesundheitsbranche, www.br.de 17.09.2019.

13 Schirrmacher, Unsicher konfigurierte Server leaken Daten von Millionen Patienten, www.heise.de 17.09.2019.

14 A/HRC/7/15, para. 13, https://www.ohchr.org/EN/Issues/Poverty/Pages/SRExtremePovertyIndex.aspx.

15 En. 14, RN 73 A/74/48037.

Pressemitteilung des Arbeitsbündnisses gegen Datenmissbrauch in der Medizin vom 01.12.2019

„Ärztliche Schweigepflicht über gesetzliche Willkür" – Arbeitsbündnis gegen Datenmissbrauch in der Medizin gebildet

Am vergangenen Samstag trafen sich in Frankfurt über 20 Datenschutz-Initiativen und zahlreiche kritische Bürger. Eingeladen hatte das Deutsche Psychotherapeuten Netzwerk. Die Teilnehmer einigten sich auf ein gemeinsames Arbeitsbündnis gegen Datenmissbrauch in der Medizin. „Es ist fünf vor zwölf. In einem Jahr sollen alle Daten gesetzlich Versicherter in einer Cloud gespeichert werden und dort nicht nur allen anderen Behandlern eines Patienten, sondern auch der Forschung zugänglich gemacht werden." so der Netzwerkvorsitzende Dieter Adler. Das Deutsche Psychotherapeuten Netzwerk warnt seit Jahren vor den weitreichenden Folgen der Speicherung von Patientendaten an einem zentralen Ort. Aber damit waren sie nicht allein. Viele Initiativen kämpfen in Deutschland für einen besseren Datenschutz der medizinischen Daten und gegen die blindwütige und unüberlegte Zwangsdigitalisierung der Medizin.

Datenskandale der letzten Jahre, besonders in jüngster Zeit, haben bewiesen, dass die Technologie bei weitem nicht so sicher ist wie versprochen. Selbst die für die Gesundheitscloud zuständige gematik GmbH – überwiegend im Staatsbesitz – musste unlängst zugeben, dass 90% der Arztpraxen unsicher angeschlossen sind – sprich für Hacker angreifbar. Das konnte der Datenschutzexperte Jens Ernst aus Schwerte nachweisen: vor laufenden Kameras des NDR hackte Ernst eine Arztpraxis im Handumdrehen – selbstverständlich mit Testdaten.

Dass die Patientendaten mit veralteter Technologie gespeichert werden sollen, hatte die Fachpresse schon lange kritisiert. Dass die jetzige Version der elektronischen Patientenakte in der Gesundheitscloud (ePA) ein Milliardengrab ist, musste vergangene Woche auch gematik-Chef Dr. Markus Leyck Dieken in einem Interview mit dem ärztlichen Nachrichtendienst eingestehen: „Damit die ePA in den meisten Arztpraxen pünktlich zum 1. Januar 2021 funktioniert, ist eine vierte Variante des Konnektors erforderlich." Der Konnektor ist ein etwa 2.800 Euro teures Verbindungselement, das den Praxisrechner über das Internet mit dem Cloudserver der Gesundheitscloud verbindet. Der muss jetzt offenbar in vielen Arztpraxen ausgetauscht werden – auf Kosten der gesetzlichen Krankenversicherungen.

Das Arbeitsbündnis gegen Datenmissbrauch in der Medizin spricht sich nicht grundsätzlich gegen die Digitalisierung aus. „Wir alle arbeiten mit Computern, speichern dort die Patientendaten ab. Bisher nur in der Praxis selbst, auf Rechnern, die selbstverständlich nicht am Internet angeschlossen sind. Jetzt sollen wir alle zwangsweise am Internet angeschlossen werden und ebenso zwangsweise die Daten unserer Patienten dort ablegen.", so der Netzwerk-Vorsitzende Dieter Adler.

In einer repräsentativen Umfrage des Psychotherapeuten Netzwerks wussten 44% der befragten Versicherten nichts von der Gesundheitscloud. 86% lehnten die zentrale Speicherung ihrer medizinischen Daten in der Cloud ab. Vergessen werden darf dabei nicht, dass in der Cloud brisante Daten gespeichert werden – mit oft weitreichenden Folgen für Betroffene. Während grippale Infekte oder eine Zahnwurzelbehandlung noch harmlos sind, können Geschlechtskrankheiten, Schwangerschaftsabbrüche, psychotherapeutische Behandlungen und Daten sowie Suchtmittel oder Alkoholabhängigkeit durchaus weitreichende Folgen haben. Nicht zu vergessen: Die Daten müssen mindestens zehn Jahre gespeichert bleiben. „Da kann schon mal eine depressive Krise, die bei einem Zwölfjährigen psychotherapeutisch behandelt wurde, vielleicht weil sich die Eltern getrennt haben, mit 21 noch zum Verhängnis werden: der junge Mensch weiß vielleicht nichts mehr davon – die Akte in der Cloud schon!"

Auch Dritte haben jetzt Interesse an den Daten angekündigt. So forderte im Juni der Verband der Betriebsärzte, die Deutsche Gesellschaft für Arbeitsmedizin und Umweltmedizin (DGAUM), die Politik auf, ebenfalls Einblick in die Gesundheitscloud zu bekommen. Damit werden Einstellungs- und Weiterbeschäftigungsuntersuchungen zum „Kinderspiel" – der Arbeitgeber kann alle Krankheiten des Arbeitnehmers lückenlos erfahren. Daten- und Persönlichkeitsschutz wird so zur Farce: Wer dem Betriebsarzt den Einblick verweigert, kann die Einstellung oder Weiterbeschäftigung vermutlich getrost vergessen. Und Schwangerschaften würden auch sofort publik. Das neugegründete Arbeitsbündnis gegen Datenmissbrauch in der Medizin will die Öffentlichkeit informieren und gleichzeitig mit Behandler- und Patientenvertretern sowie Datenschützern neue Modelle der Digitalisierung entwickeln.

Deutsches Psychotherapeuten Netzwerk – Kollegennetzwerk Psychotherapie – Berufs- und Interessenverband psychotherapeutisch Tätiger, Heckenweg 22, 53229 Bonn, Tel.: 0228 – 8505165, Email: post@dpnw.info, www.dpnw.info

Gemeinsame Pressemitteilung des Bündnisses „Gesichtserkennung stoppen" vom 9.1.2020

Bündnis fordert Verbot automatisierter Gesichtserkennung

Aktuelle Pläne des Innenministeriums müssen gestoppt werden



Bild: iStock

Ein Bündnis aus zivilgesellschaftlichen Organisationen wendet sich gegen den Vorstoß des Innenministeriums, an 135 Bahnhöfen und 14 Flughäfen automatisierte Gesichtserkennung einsetzen zu wollen. Stattdessen fordert das Bündnis „Gesichtserkennung stoppen" ein Verbot dieser hochproblematischen Technologie in Deutschland. Auch wenn eine Verbesserung der Sicherheit etwa an Bahnhöfen grundsätzlich sinnvoll erscheint, ist automatisierte Gesichtserkennung als Mittel dafür nicht nur ungeeignet, sondern hat immense negative Folgen für Millionen Passanten und Reisende.

Automatisierte Gesichtserkennung bedeutet eine permanente heimliche Personenüberwachung in öffentlichen Räumen wie Bahnhöfen oder Flughäfen. Die Körperdaten aller Vorbeilaufenden werden dabei erfasst und automatisiert mit Datenbanken abgeglichen, ohne dass die Betroffenen dies bemerken müssen. Damit greift die automatisierte Gesichtserkennung tief in die Rechte und Freiheiten von Menschen ein, wenn biometrische Körperdaten quasi im Vorbeigehen und anlasslos analysiert werden.

„Automatische Gesichtserkennung ist eine Hochrisikotechnologie", erklärt Viktor Schlüter von der Organisation Digitale Freiheit: „Hohe Falscherkennungsraten, die Diskriminierung von Frauen und People of Color und das enorme Missbrauchspotential stellen eine Gefahr für die Demokratie dar."

„Dieses unnötige und invasive Biometriesystem ist nur ein weiterer Baustein, den maschinenlesbaren Menschen zu schaffen. Allein durch das zufällige Vorbeilaufen legen wir mit unseren Körperdaten eine digitale Spur, die uns alle auch wegen der Unzuverlässigkeit der eingesetzten Algorithmen in unseren Rechten und Freiheiten einschränkt", sagte Dirk Engling, Sprecher des Chaos Computer Clubs.

„Die optische Vermessung von Gesichtern droht eine weitere Form der anlasslosen Überwachung zu werden, nur diesmal mit detaillierten Körperdaten", fügt Rainer Rehak vom Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung hinzu. „Wir müssen uns jetzt diesen gefährlichen Plänen in den Weg stellen, bevor immer mehr öffentliche Räume mit biometrischen Erkennungssystemen bestückt werden, die zudem nicht einmal mehr Sicherheit bringen."

„Der Einsatz dieser Technologie zur Überwachung des öffentlichen Raumes schränkt auch politische Teilhabe ein: Wer fürchten muss, automatisch erfasst zu werden, wird im Zweifel eher nicht an einer Demonstration teilnehmen", gibt Elisabeth Niekrenz von der Digitalen Gesellschaft zu bedenken.

Im Lichte stetig sinkender Kriminalitätsraten in Deutschland besteht nicht nur keinerlei Notwendigkeit für neue, teure und ineffiziente Überwachungsmaßnahmen zur anlasslosen Erfassung von Körperdaten von Reisenden, sondern ist es Zeit, ein Verbot dieser gesellschaftlich schädlichen Technologie in die Wege zu leiten. Ein Verbot automatisierter Gesichtserkennung in Deutschland hat bereits Vorbilder: Mehrere US-amerikanische Großstädte haben den Einsatz der Technologie durch staatliche Stellen im öffentlichen Raum aufgrund der damit verbundenen Gefahren verboten. Der Stadtrat von San Francisco etwa bezeichnete automatisierte Gesichtserkennung als „gefährliche Waffe" sowie als inkompatibel mit einer gesunden Demokratie und verbot ihren Einsatz.

Dass die teure Technik überhaupt einsatzreif ist und den erhofften Zweck erfüllt, ist zudem zweifelhaft: In einem Gesichtserkennungstest von Innenministerium und Bundespolizei im Jahr 2018 in Berlin war die Falscherkennungsrate so hoch, dass mehr als jede 200. Person fälschlicherweise erkannt wurde. Dies würde allein am getesteten Berliner Bahnhof Südkreuz zu täglich 600 Fehlalarmen führen. Der Chaos Computer Club und das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung kritisierten die unwissenschaftliche Vorgehensweise und Auswertung der Tests sowie die deutlich geschönten Testergebnisse. Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung fordert die detaillierte Veröffentlichung der Ergebnisse der vergangenen und laufenden Biometrie-Tests an Bahnhöfen, um eine wissenschaftliche Bewertung der Ergebnisse und eine öffentliche Diskussion über die Erkennungssysteme zu ermöglichen.

Das Bündnis „Gesichtserkennung stoppen" besteht aus den zivilgesellschaftlichen Organisationen Digitale Freiheit, Chaos Computer Club, Digitale Gesellschaft, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung sowie Digitalcourage.

https://www.gesichtserkennung-stoppen.de

Pressemitteilung des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V. vom 03.12.2019

Digitalisierung an Schulen – so nicht!

FIfF kritisiert Digitalpakt mit Windows 10 und Office 365

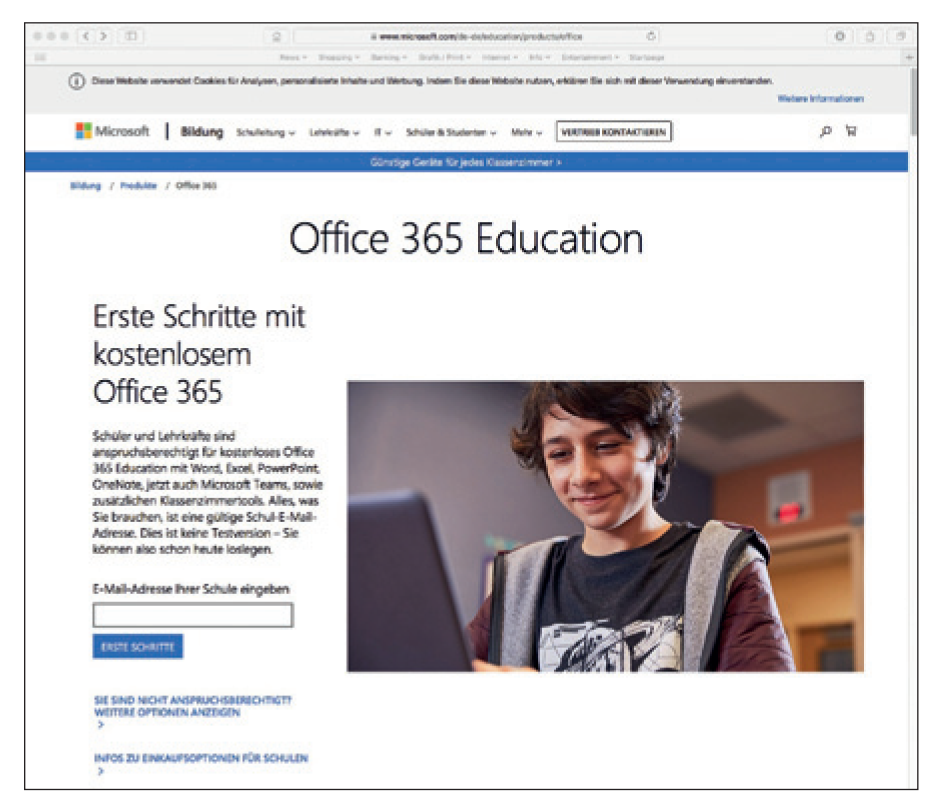
Der Digitalpakt für Schulen wurde im Mai 2019 für ganz Deutschland – trotz seines Eingriffs in die Föderalisierung – im Rahmen der Strategie für Digitalisierung durch die Bundesregierung verabschiedet. Der Bund stellt hierfür über einen Zeitraum von fünf Jahren insgesamt fünf Milliarden Euro zur Verfügung, davon in dieser Legislaturperiode 3,5 Milliarden Euro.

Aufgrund des Charakters der Bundesmittel als Finanzhilfen bringen die kommunalen und privaten Schulträger bzw. Länder zusätzlich einen finanziellen Eigenanteil ein. Zusammengenommen stehen dann insgesamt mindestens 5,55 Milliarden Euro bereit. Rein rechnerisch bedeutet dies für jede der ca. 40.000 Schulen in Deutschland im Durchschnitt einen Betrag von 137.000 Euro oder umgerechnet auf die derzeit ca. 11 Millionen Schülerinnen und Schüler eine Summe von 500 Euro pro Schüler in dem Finanzierungszeitraum.

Den Verantwortlichen, somit Schulträgern oder Schulen, steht es zunächst frei, wofür konkret sie diese Gelder zur Modernisierung der IT-Infrastruktur einsetzen. Bereits im laufenden Schuljahr 2019/2020 sollen diese Gelder abgerufen werden, um z. B. Tablets zu



Bild: iStock



kaufen. Zum funktionstüchtigen Einsatz solcher Tablets ist oftmals noch ein schulinternes WLAN zu implementieren. Mit diesen Anschaffungen und dem dauerhaften Betrieb solcher Elemente einer IT-Infrastruktur sind die Mittel pro Schüler verbraucht. Eine Hardware ohne Software ist untauglich. Als Software-Lösung sollen Verträge mit Microsoft geschlossen werden. Den meisten Schulträgern oder Schulen wird eine Lizenz von Office 365 Education unter A1 angeboten, das „Rundum-Wohlfühlpaket", welches mit dem genehmigten Digitalpakt bzw. realisierbaren Kosten für Schulen noch betrieben werden könnte.

Umfassendere Lizenzen, wie A3 oder gar A5, mit denen Verantwortliche Software-Dienste konfigurieren könnten, sind jedoch aus Kostengründen wohl kaum vermittelbar. Das FIfF kritisiert diese Lizenz-Politik und fordert, die datenschutzkonforme Verarbeitung der Daten von Schülerinnen und Schülern, die zumeist minderjährig sind. Warum wird hier nicht eine äquivalente Open-Source-Software-Lösung eingesetzt, wie sie z. B. von der Open Business Alliance angeboten wird. Mit solchen Lösungen könnten deutsche Schulen und Institutionen die Kontrolle über ihre Daten behalten, datenschutzkonforme Implementierungen leichter umsetzen und transparent die Datenschutzbestimmungen sicherstellen. Letzteres ist jedoch bei der im Rahmen der oben erwähnten Finanzierung verfügbaren Lösung mit Microsoft 365 unter A1 kaum bis gar nicht zu garantieren. Mindestens sind spezielle Regelungen in der Datenschutzgrundverordnung (DSGVO) anzuwenden, die aufbauend auf Art. 5, 6 und 7 DSGVO in Art. 8 DSGVO konkretisiert sind.

Das FIfF fordert Aufklärung, welche Interessen Microsoft verfolgt, denn die Deutsche Telekom AG hat die eigene deutsche Microsoft Cloud zum 31. August 2019 eingestellt. Das Treuhändermodell für Microsoft bei T-Systems ist damit ausgelaufen. Microsoft wird ab 14. Januar 2020 für die Betriebssysteme auf den Servern 2008 und 2008 R2 den Support einstellen und die auf ihnen laufende Software statt dessen in ihre Cloud Azure migrieren, und damit auch alle Daten in Azure in den USA stellen. Danach wird keine Kontrolle von Seiten deutscher Institutionen mehr möglich sein, und es besteht die Gefahr, dass Inhalts- und Verbindungsdaten ohne Wissen oder Genehmigung Betroffener – auch an Schulen – weiter gesammelt und per Gesetz an die NSA weitergegeben werden können. Solches hat Microsoft in anderen Zusammenhängen bereits getan.

Wie gefährlich die – schließlich lebenslang mögliche – Speicherung und Nutzung von Daten, Bildern, Medien- und App-Nutzung und alle Arten von Kommunikation für unsere Kinder ist, ist inzwischen hinlänglich bekannt geworden. Aber die Interessen und fundamentalen Rechte und Freiheiten von Kindern müssen vor allem auch an Schulen garantiert werden: Wenn ein hohes Risiko durch die Anwendung bzw. Umsetzung von Aufgaben im hoheitlichen Bereich durch IT-gestützte Prozesse in einer komplexen IT-Landschaft vorausgesetzt wird (die insbesondere nicht als IT-Landschaft vor Ort beim Schulträger oder in der Schule betrieben wird), ist eine Datenschutz-Folgenabschätzung entsprechend Art. 35 DSGVO durchzuführen. Mit einer solchen Datenschutz-Folgenabschätzung geht folglich einher, dass für Kinder bzw. Schulen technisch-organisatorische Maßnahmen höheren Anforderungen auch bzgl. der IT-Sicherheit genügen müssen. Vertraulichkeit und Integrität sind ebenso höher zu bewerten (Art. 25 und Art. 32 DSGVO). Zur Umsetzung im Besonderen auch dieser datenschutzrechtlichen Anforderungen muss verlangt werden, dass sichere Verschlüsselungen für Transport und Inhalt zu gewährleisten wären.

Das FIfF ruft dazu auf, Einspruch gegen die Regelungen des Digitalpakts einzulegen. Einsprüche gegen die derzeit bestehenden Verträge im Digitalpakt sind sachlich wie zeitlich höchst dringlich, da es Schulen jederzeit möglich ist, sich aus dem Digitalpakt zu bedienen und es bereits einzelne Schulen gibt, die dies getan haben. Was passiert, wenn ein solcher Digitalpakt und damit verbundene Nutzung von Software für Hochschulen geschlossen würde? Ähnliche Implementierungen planen Länder ja in den öffentlichen Verwaltungen, Kommunen und Städten, die ggf. auf Microsoft-Enterprise-Lizenzen basieren sollen.

Pressemitteilung des Arbeitskreises Vorratsdatenspeicherung vom 07.12.2019

Internet- und Telefonanbieter speichern Aufenthaltsort und Internetkennungen tagelang auf Vorrat



Bild: iStock

Obwohl Gerichte die umstrittene verdachtslose Vorratsdatenspeicherung ausgesetzt haben, sammeln deutsche Telekommunikationsanbieter trotzdem von jedem Kunden Informationen über ihre Kontakte und Bewegungen, die nicht zur Abrechnung nötig sind. Dies ergibt sich aus einer jetzt, aufgrund der Nachfrage des Arbeitskreises Vorratsdatenspeicherung, veröffentlichten Erhebung der Bundesnetzagentur. Die Daten werden auf Anforderung an Strafverfolger und Abmahnkanzleien weiter gegeben.

Konkret wird der Aufenthaltsort von Handynutzern (Funkzelle) zu Beginn einer Verbindung, die weltweit einmalige Kennung mobiler Endgeräte (IMEI) und die Internetkennung (IP-Adresse) eine Woche lang gespeichert, ohne dass dies zur Abrechnung nötig ist. Die im Arbeitskreis Vorratsdatenspeicherung zusammen geschlossenen Bürgerrechtler, Datenschützer und Internetnutzer warnen vor den Konsequenzen dieser „freiwilligen Vorratsdatenspeicherung“:

„Dass Mobilfunkanbieter bei jeder Verbindung den Aufenthaltsort festhalten, ermöglicht Behörden massenhafte Funkzellenabfragen und kann Unschuldige in Verdacht bringen, beispielsweise nach der Teilnahme an einer Demonstration“, erklärt Uli Breuer vom Arbeitskreis Vorratsdatenspeicherung. „Zu jeder Internetnutzung die IP-Adresse zu speichern ermöglicht Abmahnanwälten, Verbraucher tausendfach wegen angeblicher Urheberrechtsverletzungen im Internet abzukassieren, die sie oft nicht begangen haben.“

Der Arbeitskreis Vorratsdatenspeicherung verlangt von den Unternehmen, ihre „freiwillige Vorratsdatenspeicherung“ zu stoppen und die Zahl der Auskünfte über ihre Kunden zu veröffentlichen. Der Arbeitskreis Vorratsdatenspeicherung warnt außerdem, die geplante ePrivacy-Verordnung der EU drohe die „freiwillige Vorratsdatenspeicherung“ durch Telekommunikationsanbieter massiv auszuweiten, und verlangt ein klares Verbot allgemeiner und unterschiedsloser Vorratsdatenspeicherungen.

Aus Sicht der im Arbeitskreis Vorratsdatenspeicherung zusammengeschlossenen Datenschützer, Bürgerrechtler und Internetnutzer ist eine verdachtsunabhängige und wahllose Vorratsspeicherung von Telekommunikationsdaten für viele Bereiche der Gesellschaft höchst schädlich: Sie beeinträchtigt vertrauliche Kommunikation in Bereichen, in denen Menschen auf Vertraulichkeit angewiesen sind (z.B. Kontakte zu Psychotherapeuten, Ärzten, Rechtsanwälten, Betriebsräten, Eheberatern, Kinderwunschzentren, Drogenmissbrauchsberatern und sonstigen Beratungsstellen) und gefährdet damit die körperliche und psychische Gesundheit von Menschen, die Hilfe benötigen, aber auch der Menschen aus ihrem Umfeld. Wenn Journalisten Informationen elektronisch nur noch über rückverfolgbare Kanäle entgegen nehmen können, gefährdet dies die Pressefreiheit und beeinträchtigt damit elementare Funktionsbedingungen einer freiheitlichen demokratischen Gesellschaft. Die verdachtsunabhängige und wahllose Vorratsdatenspeicherung schafft Risiken des Missbrauchs und des Verlusts vertraulicher Informationen über unsere persönlichen Kontakte, Bewegungen und Interessen. Telekommunikationsdaten sind außerdem besonders anfällig dafür, von Geheimdiensten ausgespäht zu werden und Unschuldige ungerechtfertigt strafrechtlichen Ermittlungen auszusetzen.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Ungenügende Berechtigungsprüfung bei der Telematik-Infrastruktur

Am 01.01.2021 soll die elektronische Patientenakte (ePA) eingeführt werden. In dieser freiwilligen patientengeführten Akte speichern Ärzte auf Wunsch der Versicherten Befunde und Diagnosen unter Nachweis ihrer ärztlichen Identität. Der Patient soll Daten identifiziert durch seine elektronische Gesundheitskarte (eGK) im Rahmen der Telematik-Infrastruktur anderen freigeben oder sperren können. Mit einer Health Professional Card oder einer Institutionenkarte (SMC-B) soll der Nachweis geführt werden, dass Leistungserbringer, also ein Arzt, eine Arztpraxis, eine Klinik oder ein Physiotherapeut, über einen Konnektor berechtigt auf die Daten zugreift.

Auf dem 36. Chaos Communication Congress (36C3) Ende 2019 wurde offengelegt, dass das von der Anlage her sinnvolle und ausgefeilte Identitätskonzept in der realen Umsetzung schwere Lücken hat. Die notwendigen Karten für die Rollen Patient, Arzt und Institution können mit einfachen Tricks beschafft werden. Und auch der Konnektor kann über einen Versender bezogen werden, ohne dass er von einer berechtigten Institution bestellt wird. Dabei muss überhaupt nicht groß gehackt werden. Es ist gelungen, sich Zugangsberechtigungen für das Telematik-Netzwerk zu verschaffen. Es war einfach, sich die notwendigen Karten zu besorgen, mit denen das Netzwerk arbeitet.

Das fängt bei der eGK der Versicherten an, wie viele es bereits erlebt haben. Man ruft die Krankenkasse an, teilt den Verlust der Karte mit und nennt auch gleich noch die neue Adresse, zu der man gerade umgezogen ist. Ohne weitere Prüfung erhält so eine nicht befugte Person eine eGK als angeblich ausreichenden Identifikationsnachweis. Schon vier Jahre zuvor war es dem IT-Experten André Zilch gelungen, jetzt klappte es immer noch. Er ließ die Adresse eines befreundeten Versicherten per Mail bei der AOK Hessen ändern, im elektronischen Anhang ein Schreiben mit ausgedachter Unterschrift, und erhielt eine neue Karte. Die AOK Hessen erklärte, dass dies nur „unter Aufbringung krimineller Energie möglich“ sei, von „einem mühelosen unberechtigten Zugriff kann deshalb nicht die Rede sein“.

Das Vorgehen wiederholten die Hacker bei der Online-Bestellung des Institutionen-Ausweises einer Arztpraxis. Sie nahmen die notwendigen Daten von einem ärztlichen Rezept, ergänzten sie um das Geburtsdatum des Arztes aus dem Gewerberegister und unterzeichneten den ausgedruckten Antrag mit einem Gekrakel, das eine „Unterschrift“ des Arztes simulierte. Dazu wurde noch eine neue Lieferadresse genannt und das Bestellfax abgeschickt. Wenig später war die Institutionenkarte da und kurz danach kam der PIN-Brief. Der Ausweis kam per Einschreiben, die Geheimzahlen mit normaler Post. Die zuständige Kassenärztliche Vereinigung Nord räumte ein: „Jeder Besteller kann die Lieferadresse frei wählen. Dies muss nicht die Praxisanschrift, sondern kann auch eine Privatadresse sein.“

Bei der Bestellung des Arztausweises nutzten die Hacker das Bankident-Verfahren, um einen Arztausweis für Dr. med. Cyber zu bekommen. Hier muss ein Bank-Mitarbeiter zwar die Identität eines Bestellers prüfen, die Lieferadresse wird aber nicht überprüft und bestätigt. Mit ein wenig Social Engineering gelang auch dieser Schritt. Im Antrag wurde eine Passnummer erfragt. Da der Arzt, für den das Verfahren durchgeführt wurde, inzwischen einen neuen Reisepass hatte, wurde diese Nummer eingegeben, statt der hinterlegten, also eine Nummer, die weder die Bank noch die Ärztekammer kennen konnte. Offenbar erfolgte also kein Nummernabgleich. Schließlich wurde noch ein Konnektor online ohne weitere Prüfung bestellt, der mit einer besonderen „sicheren Lieferkette“ an eine nicht überprüfte Adresse geliefert wurde.

Im Antragsportal für Arztausweise von Medesign fanden die Tester der Identifizierungsverfahren eine ganze Sammlung bereits ausgefüllter Anträge, die für jeden frei einzusehen waren. In dem Datenleck fanden sich Namen, Adressen, Kontoverbindungen und Ausweisnummern sowie alles, was sonst noch nötig ist, um einen Arztausweis zu beantragen. Allein an einem Tag im Oktober 2019 waren dort Daten von 168 Ärzten zu finden, die offenbar in den beiden Wochen davor ihren Antrag gestellt hatten. Gemäß IT-Experte Martin Tschirsich spricht einiges dafür, dass auch in der Zeit davor die Anträge der jeweils letzten beiden Wochen sichtbar waren. Nachdem der Chaos Computer Club (CCC) die Lücke der Firma gemeldet hatte, reagierte die Firma prompt, so CCC-Sprecher Linus Neumann: „Das war zwar eine katastrophale Sicherheitslücke, aber die Reaktion darauf war vorbildlich. Die haben sofort geantwortet und das Leck schnellstmöglich geschlossen.“ Medesign kam nach eigenen Angaben auch seinen Meldepflichten nach. Die Antragsdaten seien regelmäßig im Abstand von vier Tagen gelöscht worden. Medesign schrieb, man habe das Identifizierungsverfahren Bankident sofort außer Betrieb genommen: „Betroffene Karten werden wir vorsichtshalber sperren.“ Die aufgeführten Schwachstellen würden nun im Detail geprüft. Die gematik erklärte die Sicherheitsmängel als „nicht hinnehmbar“. Da aber noch keine Behandlungsdaten

gespeichert würden, bestehe derzeit noch keine Gefahr für die Sicherheit der Patientendaten. Man begrüße die Aufklärung und wolle die Sicherheit gemeinsam mit dem CCC optimieren.

Rund 140.000 Praxen müssen in Deutschland an die Telematik-Infrastruktur (TI) angeschlossen werden, bei mindestens 70% ist das bereits passiert. Hinzu kommen Apotheken, Krankenhäuser sowie weitere medizinische Dienstleister. Das System wurde unter Aufsicht des Bundesamts für Sicherheit in der Informationstechnik (BSI) entwickelt. Die gematik, zuständig für den Aufbau und die Sicherheit der TI, wirbt mit dem Slogan: „Wir vernetzen das Gesundheitswesen. Sicher." Das Großprojekt sollte eigentlich schon längst vollständig in Betrieb sein. Anfang 2021 sollen im TI die elektronischen Patientenakten angelegt werden. Bundesgesundheitsminister Jens Spahn hatte Anfang 2019 angekündigt: „Ich werde bei dem Thema Gematik und elektronische Patientenakte mehr Geschwindigkeit reinbringen."

Eigentlich seien die Grundgedanken richtig, befanden Martin Tschirsich, der Arzt Christian Brodowski und André Zilch, Experte für ID-Managementsysteme bei ihrem Vortrag auf dem 36C3. Positiv sei festzuhalten, so Tschirsich, dass die gematik basierend auf den gesetzlichen Rahmenbedingungen vieles richtig macht. Es sei auch richtig, dass staatliche Stellen, Trustcenter und Ärztekammern die Basis, den Zugang zur telematischen Infrastruktur des Gesundheitswesens kontrollieren.

Doch bei der Identitätsprüfung sei bisher viel zu schlampig vorgegangen worden. Eine echte ID-Prüfung der Teilnehmer findet nicht statt, was Ausdruck einer organisierten Verantwortungslosigkeit sei: „Die rechtlich verbindliche Überführung real existierender Teilnehmer in die digitale Welt ist die zentrale Aufgabe". Zur Schadensbegrenzung führten die drei Vortragenden aus, dass unberechtigte bzw. falsch ausgestellte Zertifikate zurückgenommen werden müssen. Dann sollte ein zuverlässiger Kartenbeantragungs- und Auslieferungsservice installiert werden und eine unabhängige zentrale Prüfstelle für die Informationssicherheit der telematischen Infrastruktur eingerichtet werden, die diese Prozesse unter die Lupe nimmt.

Nach Ansicht von Tschirsich, Brodowski und Zilch hat sich die Untauglichkeit der Verfahren KammerIdent und BankIdent zur Identitätsfeststellung eines Arztes erwiesen, einzig das PostIdent-Verfahren solle übrig bleiben. Es müsse künftig strengere Restriktionen für die Auslieferung geben, was zwangsläufig den Komfort einschränkt und den Aufwand für die Beschaffung erhöht. Bisher war vorgesehen, die 55.000 Arztpraxen ohne TI-Anschluss mit Honorarabzügen von 1% zu bestrafen. Ob diese Abzüge ausgesetzt werden, solange sich neue Ärzte und Praxen mangels Zugangskarten nicht mit der TI verbinden können, wurde von der Kassenärztliche Bundesvereinigung (KBV) nicht beantwortet. Die Entscheidung hierzu liegt bei den einzelnen Kassenärztlichen Vereinigungen.

Aus dem Bundesgesundheitsministerium hieß es, die gematik werde im Januar 2020 mit den Herausgebern der Zugangskarten, also der KBV, der Bundesärztekammer und dem Spitzenverband der Krankenkassen „festlegen, wie die Prozesse sicherer gestaltet werden können". Die gematik will zudem überprüfen lassen, ob bereits Identitätsdiebstahl erfolgt ist. Es gebe aber „keinen Grund", den Zeitplan zum Aufbau des Datennetzes infrage zu stellen. Das Ministerium erklärte, es sei „gut", dass die Hacker die Lücken aufgedeckt hätten. So bleibe Zeit zu reagieren. Tschirsich reagierte, er sei froh über diese Reaktion: „Das ist der wichtigste Weg zur Besserung". Allerdings sieht er bei der TI das grundsätzliche Problem, dass „die umgesetzten Prozesse nicht gründlich genug geprüft werden". Zuvor waren auch die heutigen Verfahren als sicher eingestuft worden (Horchert/Klofta, Der Karten-Trick, Der Spiegel Nr. 1/28.12.2019, 74 f.; Borchers, 36C3: Unsichere Patientendaten – die Telematik-Infrastruktur des Gesundheitswesens hat ein Identitätsproblem, www.heise.de 27.12.2019, Kurzlink: https://heise.de/-4624092; Hoppenstedt/Ludwig, Auch der Käseladen galt als Praxis, SZ 31.12.2019/01.01.2020 S. 7; Maus, Hinweise auf mögliche Verwundbarkeiten der Medizin-Telematik, www.heise.de 17.01.2020).

Bundesweit

Weitere Hinweise auf Verwundbarkeit der Telematik-Infrastruktur

In Folge der Identifizierungsprobleme für Ärzten, Praxen und Patienten bei der Kartenausgabe für die Telematik-Infrastruktur (TI) haben sich weitere Sicherheitslücken gezeigt. Es wurden im Auftrag des Heise-Verlags bei Ärzten an deren Konnektoren nichtinvasive und nichtdestruktive Analysen durchgeführt.

-Konnektor-Probleme

Die Analysen beschäftigten sich ausführlich mit dem Modell von T-Systems, das neben dem KoCoBox-Konnektor von CGM in Praxen am weitesten verbreitet ist. Konnektoren verbinden Arztpraxen per VPN mit der TI und bilden damit das Herzstück für deren Sicherheitsarchitektur.

In der TI sollen künftig mit Einführung der elektronischen Patientenakte (ePA) ab Anfang 2021 nicht nur die Gesundheitsdaten von 73 Millionen Patienten in Deutschland verwaltet und ausgetauscht werden. Die TI soll darüber hinaus auch zur sicheren Kommunikation der Praxen und Kliniken untereinander dienen. Bislang predigen gematik und Gesundheitsministerium, dass die TI mit ihren Konnektoren und Kartenterminals „optimal sicher" sei. Probleme entstünden allein durch Nachlässigkeiten von Ärzten und deren IT-Dienstleistern, wenn sie veraltete Software nutzten und das LAN der Praxis nicht richtig absicherten.

Diese „Nachlässigkeiten" erweisen sich jedoch eher als die Regel denn als die Ausnahme. So wurden beispielsweise die von der gematik favorisierte serielle Installationen des Konnektors nur in 10% der Praxen umgesetzt. In dieser Konfiguration ist der Konnektor die einzige Verbindung der Praxis zur Außenwelt: Er baut nicht nur das

VPN zur Telematik-Infrastruktur auf, sondern dient gleichzeitig als Firewall für das Praxis-LAN Richtung Internet. Von den übrigen Praxen mit paralleler Konfiguration, bei der die Praxis ihre Internet-Verbindung in Alleinregie absichern muss, befinden sich gemäß Medienberichten rund ein Drittel in einem desolaten Sicherheitszustand.

Gemäß dem Bundesamt für Sicherheit in der Informationstechnik (BSI) „muss nach dem Stand der Technik davon ausgegangen werden, dass Leistungserbringer eine Kompromittierung eines ihrer IT-Systeme im LAN nicht sicher verhindern bzw. nicht in jedem Fall frühzeitig erkennen können." (Konnektor-Schutzprofil BSI-CC-PP-0047-2015-MA-01, Abschnitt 7.6.2). Dessen ungeachtet setzt das Schutzprofil ein unkompromittiertes Praxis-LAN für die Sicherheit der TI voraus. Hier liegt ein offenkundiger Widerspruch und ein fundamentaler Design-Fehler in der Sicherheitsarchitektur: Eine einzige kompromittierte Praxis stellt die Sicherheit vieler ePAs in Frage. Das angeblich „geschlossene medizinische Netz", welches ein „Höchstmaß an Schutz" bieten soll, ist dann eben nicht mehr geschlossen.

Wird ein Konnektor oder ein anderer Teil der TI kompromittiert, dann lassen sich womöglich nicht nur Gesundheitsdaten abgreifen und manipulieren. Angreifer könnten über in der ePA abgelegte Dokumente (darunter PDFs) auch Viren und Trojaner einspielen. Es bestünde dann Gefahr, dass sich Emotet-Angriffe, wie sie jüngst Kliniken in Fürth und Hannover lahmlegten, über die TI auf andere Praxen und Krankenhäuser ausbreiten – und das auf höchstem Sicherheitsniveau.

Selbst bei einer seriellen Konnektor-Konfiguration scheint nicht alles sicher zu sein: Der Konnektor fungiert dann nämlich gleichzeitig als Firewall für das Praxis-LAN und ist somit angriffsexponiert und sicherheitskritisch. Diesem Anspruch wird der „Medical Access Port" genannte Konnektor von T-Systems womöglich nicht gerecht. Der Konnektor wird über ein Web-Frontend konfiguriert. Der Browser des Admins ruft bei der ersten Verbindung ein Zertifikat vom Konnektor ab, das für eine verschlüsselte Verbindung (HTTPS) benötigt wird. Beim T-Systems-Konnektor produziert die Echtheitsprüfung im Browser jedoch einen Zertifikatsfehler. In allen untersuchten Praxen hatten die IT-Dienstleister (DvOs) den Ärzten geraten, die Warnung „einfach wegzuklicken".

Damit wird das Konnektor-Zertifikat ad absurdum geführt. Man-in-the-Middle-Angriffe werden ermöglicht, bei denen das Admin-Passwort abgegriffen werden kann. Angreifer in Gestalt von Patienten, Reinigungspersonal oder Lieferanten bräuchten dazu lediglich ein Gerät für unter 100 Euro im Praxis-LAN zu platzieren und könnten so Kontrolle über den Konnektor erlangen. Dagegen kann sich eine Arztpraxis mit typischer IT-Ausstattung und -Personal kaum schützen.

Das Konnektor-System basiert in großem Umfang auf Open-Source-Komponenten und würdigt dies entsprechend der Lizenzbestimmungen durch deren Benennung. Die auf der Admin-Oberfläche des Konnektors einsehbare Liste erstreckt sich über 77 Einträge. Auf sicherheitskritischen Systemen sollten niemals mehr Komponenten installiert sein als unbedingt nötig, weil sie die Angriffsfläche unnötig vergrößern. Auf dem Konnektor ist jedoch unter anderem ein WPA-Supplicant installiert, der lediglich für WLANs relevant wäre. Ebenso findet sich die E-Mail-Library mimetic, obwohl der Konnektor – zumindest offiziell – gar keine Mails verschickt. Bedenklich ist das hohe Alter einiger Komponenten: Eine xqc-Version (wahrscheinlich eine C-Schnittstelle zur XML-Query-Language) stammt offenbar vom Mai 2013, jQuery (eine populäre Bibliothek für JavaScript) vom Mai 2014.

Zudem gibt es eine Reihe von Paketen aus dem Node.js- beziehungsweise NPM-Universum auf dem sicherheitskritischen Gerät. Die Sicherheitshistorie von NPM ist ziemlich unrühmlich. Schließlich ist sogar der Paketmanager opkg dabei. Er dient dazu, Software-Pakete auf dem neuesten Stand zu halten. Auf sicherheitskritischen Geräten wie einem Konnektor dürfen aber auf gar keinen Fall irgendwelche Updates aus ungesicherten Quellen aufgespielt werden. Jedes einzelne Update muss zuvor aufwendig geprüft und zertifiziert werden. Deshalb erscheinen offizielle Firmware-Updates des Konnektors auch nur einmal im Jahr. Denn die nötige Zertifizierung nach dem internationalen Common-Criteria-Standard beschäftigt mehrere Sicherheitsprüfer über Wochen und kostet sechsstellige Beträge. Dynamische Updates wären zertifizierungswidrig.

Um einzuschätzen, wie verwundbar die auf dem Konnektor eingesetzte Software ist, wurden vom Heise-Autor zu allen Komponenten die bekannten Verwundbarkeiten herausgesucht. Diese werden in der CVE-Datenbank (Common Vulnerability Enumeration) gesammelt. Theoretisch müssten in jedem CVE-Eintrag auch die betroffenen CPE (Common Product Enumeration) aufgeführt sein. Praktisch fehlen die CPEs teils ganz oder es wird nur im Freitext erwähnt, dass die Verwundbarkeit auch in allen früheren Versionen besteht – was den Aufwand erheblich vergrößert.

Die im Konnektor von T-Systems eingesetzte Software (Firmware 1.4.13) lieferte bei einem Abgleich mit der CVEsearch-Datenbank vom 31.12.2019 sage und schreibe 3335 Treffer. Beschränkt man die Suche auf die exakten CPE-Einträge, passen immer noch 1043 Einträge, auf die sich die weitere Analyse konzentriert. Die Brisanz der Verwundbarkeiten wird nach dem CVSS (Common Vulnerability Scoring System) eingestuft. Die Skala reicht von 0 bis 10: Low (unter 4), Medium (4 bis unter 7), High (7 bis unter 9) und Critical (9 bis 10). Soweit Security-Patch-Backports plausibel zu vermuten waren – etwa beim Kernel –, wurden die entsprechenden CVEs ignoriert.

Filtert man noch alle Low-Einstufungen heraus (worüber man streiten kann), so verbleiben im T-Systems-Konnektor (Firmware 1.4.13) Hinweise auf mindestens 402 potenzielle Verwundbarkeiten: 11 kritische, 141 hochbrisante, 250 mittelbrisante (Stand 31.12.2019).

Nicht viel besser sieht es nach dem Firmware-Update aus, das T-Systems während des Untersuchungszeitraums am 28. November 2019 veröffentlichte. Die neue Firmware-Version 1.5.3 hatte am 31. Dezember immer noch 291 Hinweise auf klärungsbedürftige Verwundbarkeiten: 7 kritische, 117 hoch-

brisante und 167 mittelschwere.

Neben der bloßen Anzahl der Verwundbarkeiten alarmiert auch die Schwere einiger besonders kritischer Sicherheitslücken im CVE-Abgleich mit den Komponenten des Konnektors: Das fängt mit Anfälligkeiten für Denial-of-Service-Attacken an (CVE-2018-5391, CVE-2019-11477 und CVE-2018-5388), geht über Man-In-the-Middle-Attacken bei der Kernfunktion des VPN, weil sich die Authentifikation mit RSA bei IKEv2 unterlaufen lässt (CVE-2018-16151 und CVE-2018-16152), bis hin zu zahlreichen möglichen Pufferüberläufen, die nicht selten darin münden, dass ein Angreifer beliebigen Code ausführen kann (zum Beispiel CVE-2018-17540, CVE-2016-2108, CVE-2015-0292). Allein die in der Liste auftauchende sicherheitskritische, uralte OpenSSL-Version 0.9.8w besitzt eine kritische und fünf hochbrisante Verwundbarkeiten.

- Kartenterminals

Neben dem Konnektor kommentiert Heise auch das Kartenterminal sicherheitskritisch. Auf dessen Gehäuse kleben diverse Sicherheitssiegel des BSI, die ein unbemerktes Öffnen verhindern sollen. Ein solches Terminal ist über das Praxis-LAN mit dem Konnektor verbunden und wacht über die Verwendung der digitalen Patienten- und Arzt-Identitäten sowie über den Zugriff auf Patientendaten. Mit über hundert mittleren bis hohen sowie weiteren kritischen CVE-Einträgen, die sich seit der letzten Aktualisierung eingeschlichen haben, ist es zweifelhaft, dass das Kartenterminal ein „europaweit einzigartiges Sicherheitsniveau“ erreicht, von dem Gesundheitsministerium und gematik schwärmen.

Nicht jede in der CVE-Datenbank aufgeführte Verwundbarkeit führt zu einem tatsächlich durchführbaren Angriff. Doch für jede Verwundbarkeit, die zum Zeitpunkt der Zertifizierung bekannt ist, müsste mindestens dokumentiert sein, warum sie die Sicherheit des Systems nicht schwächen kann. Dazu dient die in der Zertifizierung vorgesehene AVA_VAN (Activity Vulnerability Assessment – Vulnerability ANalysis). Für die aufgelisteten CVE-Einträge des Konnektors und Kartenterminals existieren jedoch keine öffentlichen Dokumentationen, die deren Unbedenklichkeit nachweisen.

- Die Welt von „Common Criteria“

Das in den 90er-Jahren entstandene Zertifizierungssystem „Common Criteria“ (CC) – nach dem Konnektoren und Kartenterminals zertifiziert werden – ging noch davon aus, dass Software entweder korrekt oder aber defekt ist. Inzwischen ist klar, dass eine Komponente zum Zeitpunkt der Zertifizierung als sicher bewertet wird, weil noch niemand einen Angriffsweg entdeckt hat. Wird ein solcher Weg später publik, ist die Komponente fortan nicht mehr sicher. Im Fall eines Konnektors müsste er so lange abgeschaltet werden, bis die Unbedenklichkeit bewiesen oder die anfällige Komponente erneuert und der Angriffsweg versperrt ist. Dann könnte der Konnektor wieder weiterlaufen – bis zur Entdeckung einer neuen Verwundbarkeit.

Das Problem ist die statische Vorstellung von Programmcode in der CC-Welt, seiner Korrektheit und Sicherheit. Dies sieht man an den CC-Maintenance-Reports: Das Gerät wird als unverändert betrachtet, weswegen keine erneute Zertifizierung notwendig ist. Das Gerät mag unverändert sein, aber das Wissen über seine Sicherheitseigenschaften hat sich teils dramatisch verändert. Tatsächlich ist der Einsatz von Open-Source-Software eine gute Idee, wenn durch koordinierte Sichtungen der Quellen Verwundbarkeiten systematisch beseitigt werden. Jede CVE ist ja eine bekannte Schwachstelle, die meistens wenige Tage nach Bekanntwerden durch ein Update aus dem Verkehr gezogen wird. Von der Qualitätssicherung der CVEs kann man jedoch nur profitieren, wenn man Updates in hoher Frequenz durchführt, was innerhalb der Common Criteria kaum sinnvoll möglich ist.

Die Aussagen gelten nicht nur für den T-Systems-Konnektor. Konkurrent CGM bedient sich für seine KoCoBox MED+ ebenfalls bei Open-Source-Code. Der Hersteller listet jedoch lediglich die Lizenzen, aber nicht die Komponenten auf und verstößt somit zumindest gegen die GNU General Public License. Wenn CGM die verwendeten Open-Source-Komponenten nicht angibt, kann man für die KoCoBox vom schlimmsten Fall ausgehen, also allen Verwundbarkeiten jeglicher Software unter all den angegebenen Lizenzen. Ärzte, die den Konnektor von T-Systems einsetzen, sollten dessen Firmware – falls noch nicht geschehen – unbedingt von Version 1.4.13 auf die Ende November veröffentlichte Version 1.5.3 updaten. Dadurch können sie immerhin die Zahl der möglichen klärungsbedürftigen Verwundbarkeiten von 402 auf 291 senken. Da dies nach Ansicht des Heise-Autors nicht gut genug ist, empfiehlt er selbst bei einem aktualisierten Konnektor Ärzten nur eines: abschalten.

- Schlussfolgerung

Das sei keine pauschale Warnung vor der Digitalisierung der Medizin, sondern vor einer ungesicherten Vernetzung durch die TI. Würden Praxen und Kliniken alle digitalen Systeme mit veralteter Software abschalten, stünden Ärzte weitgehend ohne moderne Diagnostik da. Isoliert oder in Inselnetzen erzeugen aber selbst die immer noch anzutreffenden Windows-XP-Rechner zur Steuerung von Röntgengeräten kaum Gefahr – aber erheblichen Nutzen.

Die Heise-Analyse behandelt nur einen kleinen Teil möglicher Probleme der Telematik-Infrastruktur: In Bezug auf Zertifizierungsniveau oder -verfahren, Installationsqualität, Management der Authentifikationsmittel oder Updates – überall bestünden offene Fragen. So ließen sich bislang nicht einmal unabhängige Penetrationstests durchführen, weil die gematik die dazu nötigen Sandbox-Systeme nicht zur Verfügung stellt. Gesundheitsminister Jens Spahn erklärte: „Ich werde bei dem Thema gematik mehr Geschwindigkeit reinbringen, Hacker hin oder her.“ Das enorme Tempo, mit dem sein Ministerium den Ausbau der TI trotz aller Bedenken vorantreibt, ist problematisch (Maus, Hinweise auf mögliche Verwundbarkeiten der Medizin-Telematik, www.heise.de 17.01.2020, Kurzlink: https://heise.de/-4635791).

Bund

Krankenkassen-Auskunftstool „Anfrage-Generator“

Der Verein Patientenrechte und Datenschutz e.V. hat einen „Anfrage-Generator“ entwickelt, mit dem man „Krankenkassen-Auskunft mit wenigen Klicks“ erhalten können soll. Der Verein geht davon aus, dass eine Krankenkasse mehr kritische Daten über Bürgerinnen und Bürger hat als jede andere Institution: Krankheiten, Therapien, Einkommen, Arbeitsplätze, Anschriften, so der Vorsitzende Bernhard Scheffold: „Nach gegenwärtigem Stand haben Krankenkassen einen viel besseren Zugriff auf Informationen über Versicherte, als die Versicherten selbst.“ Um das zu ändern, sollen gesetzlich Versicherte über den Anfrage-Generator einfach erfahren können, was ihre Krankenkasse über sie gespeichert hat. Mit dessen Hilfe könne eine rechtskonforme Anfrage an die eigene Krankenkasse gestellt werden. Er ist unter http://kassenauskunft.de erreichbar. Über eine reine Auskunft hinaus (Art. 15 DSGVO) könne damit auch die Berichtigung falscher Daten (Art. 16 DSGVO) sowie die Löschung von Daten (Art. 17 DSGVO) verlangt werden. Scheffold erläutert: „Nur wenige Versicherte kennen ihre Rechte und die Gesetzgebung ist auf dem Weg, diese Rechte immer weiter zu beschneiden. Schon jetzt werden im Gesundheitsbereich vielfach kritische Daten verarbeitet, ohne dass die Versicherten im Einzelfall zustimmen oder auch nur widersprechen könnten.“ Der Anfrage-Generator ist Open Source, der Quelltext kann im Internet überprüft werden (https://github.com/PhilLehmann/gesundheitsdatenbefreier). Es handelt sich um ein Wordpress-Plugin („Gesundheitsdatenbefreier“), das auch andere Wordpress-Nutzer in ihren Blog einbinden können. Scheffold Ende Januar 2020: „Seit es die ersten Berichte über den Anfrage-Generator in Online-Medien und Zeitungen gab, wurden über 600 Anfragen bei den Krankenkassen damit erstellt. Benutzer haben Mängel in unseren Fehlermeldungen gefunden, die wir sofort beseitigt haben.“

Das Entwicklerteam hatte ausdrücklich darum gebeten (Patientenrechte und Datenschutz e.V. PM 15.01.2020, Krankenkassen-Auskunft mit wenigen Klicks, PM 27.01.2020, Über 600 Daten-Abfragen bei Krankenkassen in wenigen Tagen, Reges Interesse an Krankenkassen-Auskunft mit wenigen Klicks).

Bund

Umstrittener Gesetzesentwurf gegen Hasskriminalität

- Herausgabe von Passwörtern

Sicherheitsbehörden sollen gemäß einem Gesetzentwurf des Bundesjustizministeriums zur Bekämpfung der Hasskriminalität im Netz künftig das Recht erhalten, Internet-Unternehmen wie Google oder Facebook zur Herausgabe von Passwörtern ihrer Kunden zu zwingen. Durch eine Änderung des Telemediengesetzes (TMG) soll jeder E-Mail-Dienst, jedes soziale Netzwerk und jedes Unternehmen, das Dienste im Internet betreibt, verpflichtet sein, die Passwörter ihrer Kunden auf Verlangen an die Sicherheitsbehörden herauszugeben. Den Auskunftsanspruch gegen das IT-Unternehmen sollen Polizeibehörden, aber auch Verfassungsschutzämter, der Bundesnachrichtendienst und der Zoll erhalten.

Das Ministerium betonte, künftig müsse ein Richter entscheiden, ob ein Passwort angefordert werden dürfe, was eine Verschärfung darstelle. Man gehe auch nur von wenigen Fällen aus, weil Onlinedienste nach europäischem Datenschutzrecht ohnehin verpflichtet seien, Passwörter verschlüsselt zu speichern: „Dass Staatsanwaltschaften Passwörter von Diensten herausverlangen, wird daher nur in wenigen Fällen künftig geboten sein, zum Beispiel wenn es um Terrorismus-Straftaten geht und es eventuell Möglichkeiten gibt, die Passwörter mit sehr hohem technischen Aufwand zu entschlüsseln. Eine solche Pflicht für die Provider, Passwörter zu entschlüsseln, wenn Staatsanwaltschaften sie dazu auffordern, gibt es nicht und wird es auch künftig nicht geben.“ Genügen soll aber nach dem Entwurf bereits der Verdacht einer geringfügigen Straftat, die mit Kommunikationsmitteln verübt worden sein soll. Die Unternehmen sollen die Betroffenen nicht informieren dürfen, dass sie eine Passwort-Anfrage erhalten haben.

FDP-Fraktionsvize Stephan Thomae fragte: „Was ist das für eine verrückte Idee aus dem Justizministerium? Wird dort davon ausgegangen, dass die Provider meine Passwörter besitzen? Plant die Regierung entgegen dem Trennungsgebot die Einführung einer Geheimpolizei?“ SPD-Chefin Saskia Esken sieht noch Gesprächsbedarf. Bei der Frage, ob unverschlüsselte Passwörter weitergegeben werden sollten, sei man noch in der Debatte. „Das ist tatsächlich ein problematischer Punkt.“ Es gehe zwar nicht darum, Anbieter zu zwingen, Passwörter unverschlüsselt zu speichern. „Aber bei manchen Anbietern sind sie eben unverschlüsselt gespeichert. Das gehört sowieso verboten.“

Tatsächlich bekommen Cloud-Dienste nur dann eine Zertifizierung vom Bundesamt für Sicherheit in der Informationstechnologie (BSI), wenn sie Passwörter verschlüsselt speichern. Dies ist neuerdings auch laut Datenschutz-Grundverordnung geboten. Dasselbe gilt auch für die Sperrcodes von Handys. Diese sind in der Regel nur auf den Geräten und nicht auf den Servern der Unternehmen gespeichert.

Das Signal, dass der Staat prinzipiell auch auf solche Daten zugreifen möchte, hat bereits die Bürgerrechtsorganisation Gesellschaft für Freiheitsrechte (GFF) auf den Plan gerufen. Deren Vorsitzender Ulf Buermeyer kündigte an, voraussichtlich Verfassungsbeschwerde einzulegen: „Strafverfolger könnten durch die Regelung auf den Gedanken kommen, dass sie Unternehmen dazu zwingen könnten, ihre Passwörter unverschlüsselt zu speichern.“

Auf diese Kritik reagierte Bundesjustizministerin Christine Lambrecht (SPD) und kündigte an, den Entwurf zu überarbeiten und „klarzustellen“, dass auch künftig Passwörter verschlüsselt abgelegt und gespeichert werden dürfen. Die Herausgabe von Passwörtern solle „nur bei der Verfolgung schwerster Straftaten in Frage“ kommen, etwa Kindesmissbrauch, Mord und Terrorismus und von der Erlaubnis eines Richters abhängig gemacht werden.

- Meldepflicht bei Äußerungsdelikten

Die zweite geplante große Änderung für soziale Netzwerke besteht darin, dass das Justizministerium eine Anzeigepflicht für bestimmte Äußerungsdelikte festschreiben will. Unternehmen wie Facebook oder Twitter sollen verpflichtet werden, bestimmte Hasspostings ihrer Nutzer nicht nur zu löschen wie bisher, sondern sie auch an das Bundeskriminalamt (BKA) zu melden. Hierzu soll das Netzwerkdurchsetzungsgesetz verschärft werden. Auf der Liste dieser Delikte stehen unter anderem Volksverhetzung und das Verwenden verfassungsfeindlicher Symbole, das Billigen von Straftaten sowie Morddrohungen.

Im Zuge der neuen Meldepflicht sollen die Betreiber sozialer Netzwerke nicht nur verpflichtet werden, die IP-Adresse von Nutzern zu übermitteln, deren Beiträge sie gelöscht haben. Sie sollen auch die sogenannte Portnummer herausgeben. Mit dieser Nummer lassen sich verschiedene Dienste identifizieren, die über dieselbe IP-Adresse ablaufen. Hintergrund ist, dass Ermittler mit den neuen Mobilfunkstandards wie LTE oft ein Problem haben. Heute haben oft Hunderte Nutzer dieselbe öffentliche IP-Adresse, obwohl sie jeweils ein eigenes Gerät benutzen. Das liegt unter anderem daran, dass Mobilfunkprovider ihren Kunden geteilte öffentliche IP-Adressen zuweisen, weil die Adressen in dem heute am meisten verbreiteten Format knapp werden. Ein ähnliches Problem haben Ermittler, wenn Nutzer einen von mehreren Nutzern verwendeten Internetzugang wie zum Beispiel im Wifi eines Cafés nutzen. In solchen Fällen soll den Ermittlern die Portnummer helfen.

Wenn die Polizei allerdings eine Portnummer von Facebook, Google und Co. bekäme, könnten die Ermittler mit den Ziffern allein immer noch nichts anfangen. Sie müssten jetzt beim Internetanbieter, etwa der Telekom, Vodafone oder O2, anfragen, welche Person hinter der Portnummer steckt. Doch die Provider speichern diese Daten bisher gar nicht. Damit die Meldepflicht praktisch etwas bringt, müssten die Provider verpflichtet werden, auch die Portnummern zu speichern und damit viel mehr Daten über ihre Kunden speichern als bisher. Deshalb warnte der Vorsitzende des Verbandes der Internetwirtschaft eco, Oliver Süme: „Hier geht es nicht mehr nur um die Bekämpfung von Hasskriminalität, sondern um die Einrichtung umfassender Überwachungsrechte für Staat und Behörden." Kritik äußerte auch der Digitalverband Bitkom.

Keine Meldepflicht soll es weiterhin bei Beleidigung und übler Nachrede geben. Dies sind Delikte, die bislang nur auf Wunsch des Opfers verfolgt werden können. Dabei soll es auch in Zukunft bleiben. Jedoch soll für soziale Netzwerke eine neue Pflicht eingeführt werden: Wenn sich Betroffene über eine Beleidigung zum Beispiel bei Facebook beschweren, muss das Netzwerk sie darüber informieren, dass sie Strafanzeige und Strafantrag stellen können und wo sie hierüber Informationen erhalten können. Im Strafgesetzbuch werden solche sogenannten Äußerungsdelikte bislang relativ milde gewichtet.

- Erweiterte Strafbarkeit

So plant das Justizministerium nun Verschärfungen bei der Billigung von Straftaten und bei der strafbaren Bedrohung. Bislang gibt es den alten Tatbestand „Billigung von Straftaten" (§ 140 StGB – Strafgesetzbuch). Dieser Tatbestand soll erweitert werden. In Zukunft soll nicht nur bestraft werden, wer eine kriminelle Tat billigt, die schon begangen worden ist. Bestraft werden soll auch, wer eine kriminelle Tat billigt, die noch nicht begangen worden ist, also eine fiktive Tat. In letzter Zeit hat es dafür viele ernste Beispiele gegeben. Die Pegida-Anhänger zum Beispiel, die einen Galgen bastelten und mit „Angela ‚Mutti' Merkel" und „Sigmar ‚Das Pack' Gabriel" beschrifteten, kamen bisher straflos davon. Die sächsische Justiz pochte darauf, bislang habe real niemand Merkel oder Gabriel gelyncht. „Etwaige zukünftige Taten sind … nicht umfasst", schrieb die Staatsanwaltschaft Chemnitz im November 2017 in ihrem Einstellungsbescheid.

Wenn im Netz jemand schreibt, er hoffe, dass eine Person vergewaltigt werde, oder er fände es gut, wenn sie „an die Wand gestellt" würde - dann ist auch das bislang meist straflos. Auch eine Strafe wegen Bedrohung kommt dann nicht in Betracht, da der Täter vorgibt, bloßer Beobachter zu sein. Nach dem Entwurf des Justizministeriums würde die Justiz hier viel konsequenter einschreiten können und müssen.

Eine deutliche Verschärfung des Strafrechts schlägt das Bundesjustizministerium beim Paragrafen gegen Bedrohungen vor. Bislang ist nach § 241 StGB nur die Drohung mit einem Verbrechen, also einer recht schwer wiegenden Tat, strafbar. Ein Beispiel dafür ist die anonyme Drohung per Fax gegen die aus dem NSU-Prozess bekannte Frankfurter Rechtsanwältin Seda Başay-Yıldız, man werde ihre Tochter „schlachten". In Zukunft soll jegliche Drohung, also auch mit einem weniger schwer wiegenden Gewaltdelikt gegen das Opfer selbst oder eine ihm nahestehende Person, verfolgt werden können, angefangen mit einer einfachen Körperverletzung („Ich hau dich!"). Strafbar wird ebenso die Drohung mit Gewalt gegen Dinge von größerem Wert („Ich zünd dein Auto an!").

Zudem soll die Justiz diese Art von Äußerungsdelikten deutlich ernster nehmen als bisher. Bislang liegt die Höchststrafe bei einem Jahr Haft. Künftig soll sie bei öffentlichen Drohungen im Netz zwei Jahre betragen - und bei der Drohung mit einem Verbrechen, die öffentlich ausgesprochen wurde, sogar drei Jahre (Hoppenstedt/Steinke, Behörden sollen Zugriff auf Internet-Passwörter bekommen, u. Neue Wege im Kampf gegen Hass im Setz, SZ 16.12.2019, 1 u. 6; Hoppenstedt, Problemfall Passwort, SZ 17.12.2019, 5; Brühl, Lambrechts Klarstellung, SZ 29.01.2020, 5).

Bund

Bär fordert völliges Werbeprofiling-Verbot bei Kindern

Die Digital-Staatsministerin Dorothee Bär (CSU) ist bisher selten durch sinnvolle Vorschläge aufgefallen. Jetzt aber fordert sie mit guten Gründen, dass das Verwenden persönlicher Daten von Kindern und Jugendlichen für Werbung und Profilerstellung verboten wird. Sie möchte klare Regeln zum Schutz persönlicher Daten von Kindern im Internet: „Die Nutzung von persönlichen Daten

von Kindern und Jugendlichen zu Werbezwecken oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen muss klar und eindeutig verboten sein. Jugendliche und Kinder, die die virtuelle Umgebung des Internets oftmals auch als Testgebiet für die Entwicklung ihrer Persönlichkeit nutzen, sind besonders schutzbedürftig."

Der Bundesverband der Verbraucherzentralen (vzbv) hatte jüngst in einem Positionspapier zur europäischen Datenschutz-Grundverordnung (DSGVO) gefordert, das „besondere Schutzbedürfnis von Kindern" stärker zu berücksichtigen. Zwar seien in der DSGVO bereits Restriktionen für die Verarbeitung von Daten von Kindern angelegt, diese griffen jedoch oftmals zu kurz. Eine „Verarbeitung von Daten von Kindern zu Werbezwecken oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen" solle grundsätzlich ausgeschlossen sein.

Die FDP äußerte sich dazu „kritisch". Der stellvertretende Fraktionsvorsitzende Frank Sitta sagte: „Verbote sind kaum durchsetzbar und führen meistens zu Ausweichbewegungen. Daher sind Verbote und Pflichten im Netz zumeist kontraproduktiv. Viele Plattformen, die digitale Angebote bieten, reagieren bereits mit kindergerechten Versionen ihrer Produkte." Der beste Schutz für Kinder und Jugendliche sei Bildung und ein „gesunder" Umgang mit digitalen Medien im Elternhaus. Statt Verboten sprach sich Sitta für ein eigenes Schulfach für digitale Kompetenzen aus.

Bundesfamilienministerin Franziska Giffey (SPD) will bis zum Jahresende ihre Vorschläge für mehr Schutz von Kindern und Jugendlichen bei Videospielen und Apps vorlegen. Dies soll Teil des geplanten entsprechenden Jugendmedienschutzgesetzes sein. Kinder und Jugendliche sollen so besser vor Cyber-Mobbing, sexueller Belästigung und Suchtgefahr geschützt werden. Bei der Gesetzesnovelle will Giffey auch Messenger-Dienste in den Blick nehmen. Sie plädiert für sichere Voreinstellungen für Kinder und ein Meldesystem (Wittenhorst, Bär: Nutzung persönlicher Daten von Kindern zu Werbezwecken verbieten, www.heise.de 07.12.2019, Kurzlink: https://heise.de/-4607981).

Bund

Innenminister wollen Steuer-ID als Personenkennzeichen nutzen

Bei der seit Jahren in Expertenkreisen diskutierten Registermodernisierung mit einem verfahrensübergreifenden „Identitätsmanagement" machen die Innenminister von Bund und Ländern weiter Druck. In einem von der Innenministerkonferenz (IMK) veröffentlichten Zwischenbericht heißt es, dass „bis zum 1. Quartal 2020" klar sein müsse, welches Identitätsmerkmal hierzulande genutzt werden solle, um etwa Angaben zu Unternehmen, Gebäuden und Wohnungen sowie Flurstücken mit einzelnen Personen aus den Datenbeständen der Behörden zusammenzuführen: „Verlässliche Angaben zur Identität von Personen sind die Basis aller Verwaltungsleistungen. ... Wird die Verwaltung zunehmend digitalisiert, muss auch in der digitalen Kommunikation gewährleistet sein, dass Personenverwechslungen ausgeschlossen und die betroffene Person eindeutig identifiziert wird." Heißer Favorit des Hauses von Horst Seehofer (CSU) für eine einschlägige übergreifende Kennziffer ist die an sich bereits umstrittene einheitliche Steuer-Identifikationsnummer. Die „Steuer-ID" sei, so der Bericht, „der bekannteste der bereits bestehenden Identifier in Deutschland". Zusätzlich habe diese Kennung den großen Vorteil, dass das Bundeszentralamt für Steuern (BZSt) bereits in mehreren Jahren unter einigen Mühen eine darauf basierende zentrale Datenbank aufgebaut hat. Ein solches Identitätsregister sei generell nötig, „um eine registerübergreifend einheitliche Verantwortung für die Aktualität, Qualität und Konsistenz des Basisdatensatzes einer Person" mit Vor- und Nachname, Geburtsdatum und -ort, aktueller Meldeadresse und Staatsangehörigkeit „zu etablieren und einen eindeutigen Identifier zu vergeben".

Die Steuer-ID-Datenbank des BZSt enthalte keine Finanz- oder Steuerinformationen, sondern Angaben, „die der eindeutigen Identifikation einer Person dienen". Dabei würden durch Datenübermittlungen der Meldebehörden alle meldepflichtigen sowie über die Finanzämter weitere steuerpflichtige Personen erfasst. Unstimmigkeiten bei Datensätzen kläre das BZSt zusammen mit den anderen beteiligten Stellen ab. Das System spiele damit schon heute „eine wichtige Rolle bei der Qualitätssicherung der Daten in den Registern der Innenverwaltung".

Auch „Datenkranz, Personenkreis und Aufgaben der Steuer-ID-Datenbank" weisen laut den Berichtsautoren bereits jetzt einen hohen Deckungsgrad zu den Anforderungen der Innenministerkonferenz (IMK) auf. Sie heben vor allem „die große Expertise des BZSt im Bereich der Qualitätssicherung von Identitätsdaten und bei der Vergabe eindeutiger Identifikatoren" hervor, auch wenn „die wahre Identität von Personen" bisher nicht hinterfragt werde und hier noch nachgebessert werden müsse. Für erforderliche Datenübermittlungen in oder aus anderen Registern könnte ferner „weiterhin das Meldewesen seine Stärke als ‚informationelles Rückgrat der Verwaltung' ausspielen".

Datenschützer, für die ein allgemeines Personenkennzeichen ein rotes Tuch ist, bemängeln seit Langem, dass die Steuer-ID entgegen der ursprünglichen politischen Beteuerungen zunehmend in den verschiedensten Lebensbereichen verwendet wird. Banken, Versicherungen und Krankenkassen hätten das personenbezogene Merkmal für sich entdeckt, was die Gefahr der Anlage aussagekräftiger Persönlichkeitsprofile vergrößere.

Das Bundesinnenministerium sieht dagegen keine Probleme rund um die Privatheit der Bürger. Nach der Rechtsprechung des Bundesverfassungsgericht sei mit Blick auf das informationelle Selbstbestimmungsrecht zwar insbesondere durch organisatorische, technische und rechtliche Maßnahmen zu verhindern, dass alle mit dem Kennzeichen verbundenen Daten zusammengeführt werden. Ferner sei „begründet darzulegen, dass unter Berücksichtigung der verfolgten Ziele der Grundrechtseingriff im Ergebnis verhältnismäßig ist". Dies sei im Rahmen des Konzepts aber machbar.

Einschlägige rechtliche Rahmenbedingungen fänden sich in der Daten-

schutz-Grundverordnung (DSGVO) und gegebenenfalls in „ergänzenden Regelungen“, legen die Autoren dar. Diese lasse in Artikel 87 „Kennzeichen von allgemeiner Bedeutung ausdrücklich zu“. Um Risiken zu begegnen, sollten „Abhilfemaßnahmen“ aber schon bei der Konzeption durch geeignete Weichen- und Voreinstellungen im Sinne von „Privacy by Design“ berücksichtigt werden. Der IMK-Beschluss beinhalte zudem eine Maßgabe, dass die betroffenen Personen im Rahmen ihres datenschutzrechtlichen Auskunftsrechts über eine Art Cockpit „jederzeit auf einfache Weise feststellen können, welche Behörde zu welchem Zweck auf welche ihrer Daten zugegriffen hat“.

„Die fachlichen Themen und die Gestaltung der Prozesse und der Verantwortung für die neuen Verwaltungsaufgaben“ sollen laut den Innenministern bis zum Frühjahr 2020 mit einem Abschlussbericht so weit vorangebracht werden, „dass eine Entscheidung darüber getroffen werden kann“, ob das vorgesehene Identitätsmanagement über die Steuer-ID realisiert „oder eine neue Datenbank aufgebaut werden soll“. Zumindest für das Bundesressort ist dabei angesichts des „dargestellten fachlichen Mehrwerts“ der skizzierten Lösung schon klar, wohin die Reise gehen soll. Die IMK insgesamt begrüßte diese Linie Anfang Dezember auf ihrer Herbsttagung in Lübeck (Krempl, Innenminister: Melderegister sollen über die Steuer-ID vernetzt werden, www.heise.de 14.12.2019, Kurzlink: https://heise.de/-4615550).

Bund

Smart-Meter-Einführung steht vor der Tür

Nach einem mehrjährigen Vorlauf sollen in absehbarer Zeit endgültig die gesetzliche Pflichten zum Einbau intelligenter Stromzähler greifen. Eine der wichtigsten Voraussetzungen ist, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) zunächst Smart-Meter-Gateways von drei unterschiedlichen Herstellern überprüft und für gut befunden hat. Diese Auflage ist seit dem 19.12.2019 erfüllt, nachdem die Behörde das dritte einschlägige Zertifikat an die Firma EMH Metering übergeben hat. Zuvor hatten die Unternehmen Power Plus Communications und OpenLimit SignCubes gemeinsam Ende 2018 sowie Sagemcom Dr. Neuhaus im September 2019 erfolgreich das aufwändige Zertifizierungsverfahren durchlaufen. Dabei evaluierte das BSI neben den Sicherheitsvorgaben in den Geräten selbst auch die Herstellungs- und Entwicklungsprozesse der Produzenten sowie die Auslieferungswege der Systeme. Sieben weitere Gateways befinden sich noch im Zertifizierungsverfahren.

Im Herbst hatte das BSI zudem auch drei dazugehörige Sicherheitsmodule der Unternehmen NXP/T-Systems, STMicroelectronics und Gemalto offiziell gebilligt. Ferner hatte die Behörde bis dahin bei 38 Unternehmen festgestellt, dass sie die Vorgaben für den sicheren Betrieb von Gateways umgesetzt haben, sowie 10 Zertifizierungsdienstleister für die einschlägige Public-Key-Infrastruktur (PKI) registriert.

BSI-Präsident Arne Schönbohm sprach von einem „wichtigen Schritt hin zu einer erfolgreichen Digitalisierung der Energieversorgung in Deutschland“. Seine Prüfer hätten gezeigt, „dass innovative Technik und Informationssicherheit dabei Hand in Hand gehen“ und die Privatsphäre der Verbraucher geschützt sei. Für die breite Einführung der Technik gemäß dem Messstellenbetriebsgesetz fehlt nun noch eine erneute Marktanalyse des BSI, in der diese die technische Möglichkeit eines flächendeckenden Betriebs intelligenter Stromzähler feststellen muss. Dieser abschließende Schritt soll laut der Behörde – etwas verzögert – Anfang 2020 erfolgt sein. In der sogenannten Markterklärung sollen „die besonderen Anforderungen unterschiedlicher Einsatzbereiche“ mit den technischen Gegebenheiten abgeglichen werden. Ende Januar 2019 hatte das BSI bereits in der Vorjahresanalyse konstatiert, dass die für den verschlüsselten Einsatz intelligenter Messsysteme nötige Infrastruktur ausnahmslos verfügbar sei. Seitdem war der freiwillige Einbau von zertifizierten Geräten prinzipiell möglich. Die kommende Pflicht besteht für Haushalte mit einem Jahresstromverbrauch von über 6.000 kWh, was durchschnittlich mit fünf oder mehr Personen erreicht sein dürfte.

Smart Meter werden auch vorgeschrieben, wenn Solaranlagen mit einer Leistung von sieben bis 100 Kilowatt installierter Leistung Strom erzeugen oder Verbraucher ein verringertes Netzentgelt für eine Wärmepumpe oder eine Nachtspeicherheizung zahlen beziehungsweise über eigene Ladepunkte für Elektromobile verfügen. Für Haushalte mit einem Jahresverbrauch unter der festgelegten Grenze kann der Einbau trotzdem obligatorisch werden, wenn der Messstellenbetreiber oder der Vermieter Nägel mit Köpfen machen.

Der Verbraucherzentrale Bundesverband (vzbv) befürchtet, „dass Verbraucher auf Zusatzkosten sitzen bleiben“. Theoretisch seien Smart Meter zwar eine gute Sache, da sie „die Energiewende voranbringen sollen“. Die Netz- und Messstellenbetreiber müssten aber auch variable Tarife anbieten und eingesparte Kosten vollständig weitergeben. Smart Meter der ersten Generation seien zudem technisch nicht in der Lage, Photovoltaikanlagen und Ladestationen für E-Fahrzeuge je nach Netzauslastung selbstständig zu steuern. Dafür seien weitere Geräte erforderlich. Laut einer im Auftrag des vzbv vom Hopp-Marktforschungsinstitut durchgeführten repräsentativen Umfrage sind 69% der Verbraucher der Meinung, dass intelligente Stromzähler nur eingebaut werden sollten, wenn die Kosteneinsparung durch weniger Energieverbrauch etwa die Einbau- und Betriebsgebühren übersteigt.

Die Grünen im Bundestag wollen derweil Konsumenten mehr Souveränität bei Strombezug und -verbrauch einräumen. In einem Antrag fordert die Fraktion eine Garantie, dass Haushaltskunden von der Smart-Meter-Einführung „in der Regel finanziell profitieren“. Die Chancen der Digitalisierung für die Energiewende müssten besser genutzt, Anwendungsmöglichkeiten der Gateways erweitert werden. Die Piraten rufen dagegen schon seit Längerem zum Widerstand gegen die Zwangsbeglückung der privaten Verbraucher mit „Spionagezählern“ auf (Krempl, Intelligente Stromzähler: Pflicht zum Smart-Meter-Einbau soll Anfang 2020 greifen, www.heise.de 23.12.2019, Kurzlink: https://heise.de/-4623221).

Bund

BSI warnt vor „Emotet" verseuchten Behörden-Mails

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnte Mitte Dezember 2019, dass im Namen des Staates gegen dessen Willen gefährliche E-Mails verschickt werden. Mehrere Bundesbehörden wurden vom mächtigen Botnet „Emotet" infiziert. Bürger sollten besonders vorsichtig sein, wenn sie E-Mails von Behörden bekämen. Über Anhänge und Links in solchen E-Mails könnten Bürger ihre eigenen Computer infizieren. Das BSI warnt davor, solche E-Mails und Links zu öffnen. Sollte ein Mitarbeiter eines Unternehmens eine verdächtige E-Mail oder einen verdächtigen Anhang schon geöffnet haben, solle er seinen IT-Sicherheitsbeauftragten informieren.

Dem BSI waren zuvor mehrere bestätigte Emotet-Infektionen in Behörden der Bundesverwaltung gemeldet worden. Emotet hatte E-Mail-Adressen und ganze Mail-Verläufe der Behörden ausgelesen und versuchte dann, diese als Tarnung zu nutzen, um weitere Computer zu infizieren: Das BSI weist darauf hin, dass die Angreifer ihre Technik in den vergangenen Jahren mehrfach weiterentwickelt haben: „Damit gelingt es Emotet, eine sehr weite ungezielte Verbreitung zu erreichen, die andere Spam-Kampagnen bei weitem übersteigt. Emotet gilt derzeit als die gefährlichste Schadsoftware der Welt." CERT-Bund, das Computer-Notfallteam des BSI für die Bundesverwaltung, warnte auf Twitter: „Sei nicht der Nächste". Das Amt spricht von „hochkarätigen Opfern" der Software. Schaden in den Behörden selbst sei nicht angerichtet worden. Es handele sich um Erstinfektionen, die dazu führten, dass weitere Spam-Mails im Namen der Betroffenen verschickt würden. Das BSI bereinigte die infizierten Systeme. Dem Amt zufolge ist es die erste größere Emotet-Infektion in den Bundesbehörden.

Entdeckt wurde Emotet 2014, damals wurde es vor allem als Banking-Trojaner verwendet. Einmal von ahnungslosen Menschen installiert, stahl das Programm die Zugangsdaten zum Konto, wenn der Nutzer an sein Online-Banking wollte. Heute können Cyberkriminelle über Emotet weitere Schadsoftware auf infizierte Rechner nachladen, darunter den Banking-Trojaner Trickbot, der Kontos knacken soll, oder Ransomware wie Ryuk, die Dateien verschlüsselt und Lösegeld fordert, um die Dateien wieder verwendbar zu machen (Gefahr per Mail, SZ 19.12.2019, 5).

Bund

1&1 soll 9,5 Millionen Euro Strafe zahlen

Der Bundesdatenschutzbeauftragte (BfDI) Ulrich Kelber hat gegen die Telekommunikationsfirma 1&1 ein Bußgeld in Höhe von 9,55 Millionen Euro verhängt. Der Telekommunikationsdienstleister, zu dessen Konzernverbund auch die von dem Fall nicht betroffenen Mail-Anbieter Web.de und GMX gehören, hatte Kelber zufolge „keine hinreichenden technisch-organisatorischen Maßnahmen" zum Schutz von Kundendaten ergriffen. Die Aufsichtsbehörde wirft der Firma vor, dass Unberechtigte an der Telefon-Hotline vergleichsweise einfach „weitreichende Informationen zu weiteren personenbezogenen Kundendaten" erhalten konnten. Die Angabe von Namen und Geburtsdatum von Betroffenen hätten ausgereicht. In diesem Authentifizierungsverfahren sieht der BfDI einen Verstoß gegen Artikel 32 DSGVO, wonach Unternehmen geeignete technische und organisatorische Maßnahmen ergreifen müssen, um die Verarbeitung personenbezogener Daten systematisch zu schützen.

1&1 zeigte sich Kelber zufolge „einsichtig und äußerst kooperativ". In einem ersten Schritt habe der zu Drillisch gehörende Konzern zunächst den Authentifizierungsprozess durch die Abfrage zusätzlicher Angaben stärker abgesichert. Ferner werde derzeit nach Absprache mit der Aufsicht „ein neues, technisch und datenschutzrechtlich deutlich verbessertes Authentifizierungsverfahren eingeführt". Trotz der raschen Anpassungen hielt Kelber es für geboten, die millionenschwere Geldbuße zu verhängen. Der Verstoß habe ein Risiko für den gesamten Kundenbestand dargestellt. Die Höhe der Strafe bewege sich aufgrund des kooperativen Verhaltens von 1&1 im unteren Bereich des möglichen Bußgeldrahmens. Das Unternehmen selbst betont aktuell auf seiner Startseite im Web: „Ihre Privatsphäre ist uns wichtig! Der Schutz ihrer persönlichen Daten hat für 1&1 oberste Priorität."

Parallel hat der BfDI in einem weiteren Verfahren den Telekommunikationsanbieter Rapidata mit einem Bußgeld in Höhe von 10.000 Euro belegt. Dies sei erforderlich gewesen, da die Firma ihrer „gesetzlichen Auflage nach Artikel 37 DSGVO zur Benennung des betrieblichen Datenschutzbeauftragten trotz mehrmaliger Aufforderung nicht nachgekommen ist". Bei der Höhe der Sanktion habe man berücksichtigt, dass es sich um ein „Kleinstunternehmen" handele.

Die Behörde untersucht „aufgrund von eigenen Erkenntnissen, Hinweisen und auch Kundenbeschwerden zudem derzeit die Authentifizierungsprozesse weiterer Anbieter von Telekommunikationsdienstleistungen". Die 1&1 Telecom GmbH kündigte an, gegen den „absolut unverhältnismäßigen" Bußgeldbescheid zu klagen. Es habe sich um einen Einzelfall aus dem Jahr 2018 gehandelt, bei dem es „um die telefonische Abfrage der Handynummer eines ehemaligen Lebenspartners" gegangen sei. Die zuständige Mitarbeiterin habe dabei alle Anforderungen der damals bei 1&1 gültigen Sicherheitsrichtlinien erfüllt. Zu diesem Zeitpunkt sei eine Zwei-Faktor-Authentifizierung üblich gewesen, einen einheitlichen Marktstandard für höhere Sicherheitsanforderungen habe es nicht gegeben. In den nächsten Tagen werde man als eines der ersten Unternehmen der Branche jedem Kunden eine persönliche Service-PIN bereitstellen. Die Datenschutzbeauftragte von 1&1, Julia Zirfas, monierte, dass die Mitte Oktober 2019 eingeführte neue Bußgeldlogik der hiesigen Aufsichtsgremien „gegen das Grundgesetz" verstoße. Diese orientiere sich am jährlichen Konzern-Umsatz. So können bereits kleinste Abweichungen „riesige Geld-

bußen zur Folge haben“ (Krempl, DS-GVO-Verstoß: 1&1 muss knapp 10 Millionen Euro Strafe zahlen, www.heise.de 09.12.2019, Kurzlink: https://heise.de/-4608676).

Bundesweit

Aufsichtsbehörden legen Bußgeldmodell vor

Die deutschen Aufsichtsbehörden haben am 14.10.2019 ein Berechnungsmodell verabschiedet, wonach die Bußgeldzumessung bei Datenschutzverstößen für Unternehmen in fünf Schritten erfolgen soll: 1. Bestimmung Größenklasse; 2. Bestimmung mittlerer Jahresumsatz; 3. Ermittlung wirtschaftlicher Grundwert; 4. Multiplikation des Grundwerts mit Faktor X (Schwere der Tatumstände); 5. Anpassung anhand täterbezogener und sonstiger Umstände (Handsteuerung). Von einigen Datenschutzbehörden wurde angekündigt, dass die bisherige milde Bußgeldpraxis ein Ende haben werde (s.u., auch unter Berlin zu Deutsche Wohnen; Bußgeldberechnungskonzept: https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf).

Bundesweit

Datenschutz-Bußgelder steigen drastisch

Im Jahr 2019 sind in Deutschland mindestens 185 Bußgelder wegen Datenschutz-Verstößen verhängt worden, im Vorjahr waren es 40. Eine Umfrage des „Handelsblatts“ unter den Datenschutzaufsichtsbehörden der Länder ergab, dass seit dem Start der DSGVO im Mai 2018 225 Bußgelder ausgesprochen wurden. Im bevölkerungsreichsten Land Nordrhein-Westfalen wurden 2019 demnach 64 Bußgelder (2018: 33) verhängt, in Berlin 44 (2018: 2), in Niedersachsen 19 (2018: 0), in Baden-Württemberg 17 (2018: 2). Das Saarland sprach in sechs Fällen Bußgelder aus (2018: 1). Mecklenburg-Vorpommern hatte keine Angaben gemacht (Drastische Steigerung, SZ 02.01.2010, 27).

Baden-Württemberg

DSGVO in Kommunen bisher nur bedingt angekommen

Eine Umfrage unter Gemeinden in Baden-Württemberg zeigt, dass die meisten Kommunen mit der Umsetzung der Anforderungen der europäischen Datenschutz-Grundverordnung (DSGVO) noch hadern. Sie fühlen sich stark belastet, da Personal und Zeit fehlen. Zu diesem Ergebnis kommt eine vom baden-württembergischen Landesdatenschutzbeauftragten Stefan Brink durchgeführte Umfrage, an der sich 87% der rund 1.100 Gemeinden beteiligten.

2% der Gemeinden haben danach die Umsetzung der DSGVO bereits abgeschlossen. 25% haben alle relevanten Prozesse zumindest angestoßen, 32% die Hälfte der relevanten Prozesse, allerdings 39 % der Gemeinden mit der Umsetzung „gerade erst begonnen“. Ein Verarbeitungsverzeichnis haben 28% der Gemeinden noch nicht erstellt, 76% haben sich noch nicht mit der Frage der Datenschutz-Folgenabschätzung befasst. 11% hingegen haben bei den Informationsrechten und 14% bei den Betroffenenrechten Nachholbedarf.

Stefan Brink meinte, es bestehe „vor allem bei kleineren Gemeinden der Eindruck, den Anforderungen der Datenschutz-Grundverordnung sei mit der Bestellung eines Datenschutzbeauftragten bereits genüge getan“. 78% der Gemeinden haben einen externen Datenschutzbeauftragten, die meisten beim gleichen Anbieter. Dessen Betreuung wird „oft als nicht zufriedenstellend“ bezeichnet. Brink sieht den Hauptgrund im Betreuungsschlüssel: „Ein hauptamtlicher externer Datenschutzbeauftragter sollte nicht mehr als 15 bis 20 Gemeinden betreuen.“

Insbesondere im Bereich der Datensicherheit gebe es „häufig ungenügende Zustände“. Hier muss, so der Landesbeauftragte, „dringend nachgebessert“ werden. So gaben 48% der Gemeinden an, ihre Laptops nicht zu verschlüsseln, bei Desktop-Computern sind es 57%. Überdies binden über die Hälfte der kommunalen Websites Elemente von Dritten ein, etwa Google oder Facebook, wozu Brink klarstellte: „Dafür gibt es keine Rechtsgrundlage.“ Nur wenige Gemeinden bieten den Bürgern die Möglichkeit, sicher per Ende-zu-Ende-Verschlüsselung mittels E-Mail zu kommunizieren. Am häufigsten kommt dabei der Dienst De-Mail zum Einsatz. Entsprechend melden die Gemeinden bei der Datenschutzaufsichtsbehörde einen „sehr hohen“ Bedarf an Beratung und Unterstützung an. Diese können beispielsweise geschehen durch Schulungen, Mustervorlagen oder Handreichungen. Die Behörde stellt deshalb nun auch eine neue Broschüre „Datenschutz bei Gemeinden“ zur Verfügung (Schulzki-Haddouti, Kommunen ächzen unter der Datenschutz-Grundverordnung, www.heise.de 05.11.2011, Kurzlink: https://heise.de/-4578358, Umfrageergebnisse unter https://www.baden-wuerttemberg.datenschutz.de/gemeinden-umfrage/).

Bayern

Linke fordern in Erlangen Ehrenbürgerwürde für Chelsea Manning

Die Stadtratsgruppe „erlanger linke“ hat November 2019 in einem Antrag im Rat der Stadt Erlangen gefordert, die Whistleblowerin und „politische Gefangene der USA“ Chelsea Manning zur Ehrenbürgerin zu machen. Sie habe Beweise über Kriegsverbrechen der US-Army, unter anderem das Beweisvideo „collateral murder“, und über Guantanamo veröffentlicht – dafür ist sie zu 30 Jahren Haft verurteilt worden. Nach der Begnadigung durch US-Präsident Barack Obama kurze Zeit frei, wurde sie in Beugehaft genommen, um sie dazu zu zwingen, Julian Assange von Wikileaks zu belasten, dem in den USA möglicherweise die Todesstrafe drohe. Manning werde nicht aussagen, auch wenn das weitere Jahre im Gefängnis bedeute. Für die Linken ist sie eine politische Gefangene, die Solidarität und Respekt für ihre mutige und konsequente Haltung verdiene. Die Stadtratsgruppe hatte vorher die Zustimmung von Chelsea Manning eingeholt, und will den Rat dazu bringen, ihren Antrag öffentlich zu behandeln (PM erlanger linke, 16.11.2019).

Berlin

14,5 Mio.-Bußgeldbescheid gegen Deutsche Wohnen

Die Immobiliengesellschaft Deutsche Wohnen SE hat wegen Verstoßes gegen die Datenschutz-Grundverordnung ein Bußgeld von 14,5 Mio. € von der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) auferlegt bekommen. Deutsche Wohnen hat, wie sich bei Prüfungen vor Ort im Juni 2017 und im März 2019 ergab, für die Speicherung personenbezogener Daten von MieterInnen ein Archivsystem verwendet, das keine Möglichkeit vorsah, nicht mehr erforderliche Daten zu entfernen. Personenbezogene Daten seien gespeichert worden, ohne zu überprüfen, ob eine Speicherung zulässig oder überhaupt erforderlich ist. In Einzelfällen hätten teilweise Jahre alte private Angaben betroffener Mieter eingesehen werden können, ohne dass diese noch dem Zweck ihrer ursprünglichen Erhebung dienten. Es habe sich dabei beispielsweise um Gehaltsbescheinigungen, Selbstauskunftsformulare, Auszüge aus Arbeits- und Ausbildungsverträgen, Steuer-, Sozial- und Krankenversicherungsdaten sowie Kontoauszüge gehandelt.

2017 hat die Behörde der Datenschutzbeauftragten (BlnBDI) Maja Smoltczyk gemäß eigenen Angaben dem Unternehmen dringend empfohlen, das Archivsystem umzustellen. Im März 2019 hatte Deutsche Wohnen weder den Datenbestand bereinigt noch rechtliche Gründe vorgewiesen, die Daten weiter zu speichern. „Zwar hatte das Unternehmen Vorbereitungen zur Beseitigung der aufgefundenen Missstände getroffen. Diese Maßnahmen hatten jedoch nicht zur Herstellung eines rechtmäßigen Zustands bei der Speicherung personenbezogener Daten geführt." Daher sei wegen eines Verstoßes gegen Artikel 25 Abs. 1 DSGVO sowie Artikel 5 DSGVO ein Bußgeld fällig.

Smoltczyk erklärte: „Datenfriedhöfe, wie wir sie bei der Deutsche Wohnen SE vorgefunden haben, begegnen uns in der Aufsichtspraxis leider häufig. Die Brisanz solcher Missstände wird uns leider immer erst dann deutlich vor Augen geführt, wenn es, etwa durch Cyberangriffe, zu missbräuchlichen Zugriffen auf die massenhaft gehorteten Daten gekommen ist. Aber auch ohne solch schwerwiegende Folgen haben wir es hierbei mit einem eklatanten Verstoß gegen die Grundsätze des Datenschutzes zu tun." Die Bußgeldentscheidung ist nicht rechtskräftig. Das Unternehmen hat seinen Sitz in Berlin und betreibt 165.500 Wohneinheiten und 2.700 Gewerbeeinheiten. Die Deutsche Wohnen SE hat gegen den Bußgeldbescheid Einspruch eingelegt.

Seitdem die Bußgeldvorschriften der DSGVO bekannt sind, wird in Deutschland eine Diskussion um die Höhe bzw. Erhöhung von Bußgeldern geführt. Die in der Vergangenheit von deutschen Aufsichtsbehörden verhängten Bußgelder waren überschaubar. Laut Pressemeldungen aus dem Mai 2019 gab es 7 Fälle in Baden-Württemberg mit einem Gesamtbußgeld von 203.000 EUR, 9 Fälle in Rheinland-Pfalz mit einem Gesamtbußgeld von 124.000 EUR, 18 Fälle in Berlin mit einem Gesamtbußgeld von 105.600 EUR, 2 Fälle in Hamburg mit einem Gesamtbußgeld von 25.000 EUR, 36 Fälle in Nordrhein-Westfalen mit einem Gesamtbußgeld von 15.600 EUR und 3 Fälle im Saarland mit einem Gesamtbußgeld von 590 EUR (s.o. die Meldungen zu Bußgeldern unter Bund und Bundesweit, Wilkens, Verstoß gegen DSGVO: Deutsche Wohnen soll 14,5 Millionen Euro zahlen, www.heise.de 05.11.2019, Kurzlink: https://heise.de/-4578269; Deutsche Wohnen wehrt sich, SZ 19.11.2019, 19).

Berlin

Smoltczyks Gesprächsbedarf wegen Greta-DB-Dialog

Ein reger Twitter-Dialog zwischen der Klimaaktivistin Greta Thunberg und der Deutschen Bahn veranlasste die Berliner Datenschutzbeauftragte Maja Smoltczyk, mit der Bahn über den Umgang mit „personenbezogenen Reisedaten" zu sprechen. Das Thema solle unabhängig vom Einzelfall besprochen werden, sagte ein Sprecher Smoltczyks. Weder lägen Beschwerden vor, noch sei ein Verfahren gegen das Unternehmen geplant: „Wir sehen es aber generell kritisch, wenn die Bahn Daten von Reisenden veröffentlicht."

Eine Zugfahrt Thunbergs hatte am Wochenende des 3. Advent für Aufsehen gesorgt. Die 16-Jährige hatte am Samstag bei Twitter ein Foto gepostet, das sie auf dem Boden sitzend zwischen Koffern in einem ICE zeigt. Dazu hatte sie geschrieben: „In überfüllten Zügen durch Deutschland. Und ich bin endlich auf dem Heimweg!" Sie war nach monatelanger Reise auf dem Rückweg nach Schweden. Die Bahn twitterte daraufhin, Greta sei im ICE 74 zwischen Kassel und Hamburg auch in der Ersten Klasse gereist und auf ihrem Sitzplatz vom Zug-Team betreut worden. Thunberg erklärte daraufhin, ihr Zug von Basel aus sei ausgefallen, weshalb sie im Anschluss in zwei Zügen auf dem Boden gesessen habe. Dann habe sie einen Sitzplatz erhalten.

Die Deutsche Bahn erhalte aus den Buchungssystemen keine Fahrgastdaten, erklärte eine Sprecherin zur Ankündigung der Berliner Datenschützerin. „Im vorliegenden Fall hat die DB auf Nachfrage von Journalisten mit dem Bordpersonal des Zuges gesprochen, mit dem Greta Thunberg fuhr." Rechtsgrundlage sei ein berechtigtes Unternehmensinteresse laut Datenschutz-Grundverordnung (Datenschutzbeauftragte klopft an, Fehde mit Thunberg verfolgt Deutsche Bahn, www.n-tv.de 18.12.2019).

Berlin

Smoltczyk: „berlin.de" verletzt Datenschutz

Berlins Datenschutzbeauftragte Maja Smoltczyk erhob am 09.12.2019 im Berliner Abgeordnetenhaus schwere Vorwürfe gegen die Betreiberfirma des Hauptstadtportals berlin.de (Berlin Online). Die Firma gehört zu 74,8% dem Berliner Verlag (mit seinen neuen Eigentümern Silke und Holger Friedrich) sowie zu 25,2% der landeseigenen Investitionsbank Berlin (IBB). Diese handle für das Land Berlin „rufschädigend" und aus Datenschutz-Perspektive „absolut inakzeptabel".

Smoltczyk reibt sich vor allem daran, dass Berlin Online Daten von Besuchern

des deutschlandweit am häufigsten geklickten Stadtportals erhebe und verarbeite, ohne dass diese davon Kenntnis hätten oder einwilligten. Sie bezog sich damit auf Werbe-Tracker auf dem privaten Auftritt von Berlin Online mit einem Nachrichtenportal, wo die Betreiberfirma Banner schaltet. Diese Instrumente sammeln Daten von Nutzern, die zu Profilen verdichtet werden können und eine zielgerichtete Ansprache von Verbrauchern ermöglichen sollen.

Eine Studie des dänischen Dienstleisters Cookiebot hatte im März 2019 ergeben, dass etwa ein Übersichtsartikel zu Strategien gegen Alkoholsucht auf berlin.de Informationen über die Nutzenden an 20 verschiedene Tracking-Domains lieferte. Smoltczyk teilte den Abgeordneten im Ausschuss für Kommunikationstechnologie mit, dass sie die Datensammelpraxis auf dem Portal überprüfe. Es habe mehrere Beschwerden über die Seite gegeben. Der Bundesdatenschutzbeauftragte Ulrich Kelber hatte angekündigt, dass die deutschen Aufsichtsbehörden bei Web-Tracking ohne informierte Einwilligung der Betroffenen verstärkt „verwarnen, untersagen“ und von Bußgeldern Gebrauch machen wollten. Smoltczyk bezeichnete es als bedenklich, dass Nutzer zwischen dem wirtschaftlich ausgerichteten Teil und dem für das Land Berlin bereit gestellten offiziellen öffentlichen Webangebot etwa mit Pressemitteilungen des Senats nicht unterscheiden könnten. Die Hoheit über die Verwendung eigener Daten gehe dem Besucher der Seite so verloren.

Holger Friedrich hatte das Onlineportal zuvor in einem Interview als den „eigentlichen Schatz unseres Deals“ ausgemacht. Die Seite solle „der Hebel, die zentrale Plattform“ werden, skizzierte der Internetunternehmer und Neu-Verleger die Pläne des Paars. Seine Frau ergänzte, dass die Betreiber dort „prinzipiell jede Dienstleistung ausspielen“ könnten. Über eine App mit Ausweisprüfung und Abgleich der Steueridentifikationsnummer sollten nach den Vorstellungen der Friedrichs zahlreiche Bürgerdienste online angeboten werden. Der Senat betonte dagegen, den Vertrag mit Berlin Online bereits 2018 gekündigt zu haben, also schon „bevor die neuen Eigentümer den Verlag übernommen haben“. Die Zusammenarbeit ende im Dezember 2021. Die IBB soll dann voraussichtlich die Betreiberfirma komplett übernehmen.

Der Geschäftsführer von Berlin Online, Olf Dziadek, hatte im Vorfeld der Ausschuss-Sitzung Vorwürfe ungerechtfertigter Datenerhebungen zurückgewiesen. Abgeordnete von SPD, Linken und der oppositionellen CDU stellten dagegen selbst eine fortgesetzte Zusammenarbeit zwischen dem Land Berlin und dem Unternehmen bis zum Vertragsende in Frage. Das Portal müsse auf jeden Fall datenschutzkonform betrieben werden (Krempl, Werbe-Tracking: Datenschutzbeauftragte prüft Landesportal berlin.de, www.heise.de 10.12.2019, Kurzlink: https://heise.de/-4609895).

Hamburg

Transparenzgesetz verschlimmbessert

Die Freie und Hansestadt Hamburg galt mit dem 2012 in Kraft getretenen Transparenzgesetz lange als Vorbild für Informationsfreiheit auch in anderen Bundesländern. Nun erhält dieses Image Kratzer mit einer Reform der Bestimmungen für das „gläserne Rathaus“, die die Bürgerschaft der Hansestadt Mitte Dezember 2019 ohne weitere Aussprache mit den Stimmen der Regierungsfraktionen von SPD und Grünen sowie CDU und FDP beschlossen hat. Demnach sollen Ämter künftig Namen und Anschrift von Antragstellern auf Akteneinsicht gegenüber Betroffenen in einigen Bereichen offenlegen. Der ursprüngliche, von den Abgeordneten noch in einigen Punkten überarbeitete Entwurf des Senats war an diesem Punkt noch schärfer gefasst gewesen. Er sah bei Auskunftsanträgen, die personenbezogene Daten, Betriebs- und Geschäftsgeheimnisse oder „das geistige Eigentum Dritter“ berühren, eine Pflicht vor, auf Nachfrage Dritten gegenüber die Identität des Anfragenden zu offenbaren.

Gegen diese Initiative waren Bürgerrechtsorganisationen Sturm gelaufen, da sie Medienvertreter und die Pressefreiheit in Gefahr sahen. „FragdenStaat“ warnte, dass so auch Daten von Journalisten, die „Anfragen zu zwielichtigen Unternehmen oder Rechtsextremen an die Verwaltung stellen‘“, bei ebendiesen landen könnten. Der investigative Reporter Ján Kuciak sei voriges Jahr in der Slowakei ermordet worden, nachdem eine Behörde seine Adresse bei einer Informationsanfrage weitergegeben habe. Der Hamburgische Informationsfreiheitsbeauftragte Johannes Caspar bestätigte: „Hier ist absolute Vorsicht geboten. Es darf nicht sein, dass der Anfragende mit seinen Daten für die Auskunft bezahlen muss.“

Mit den Korrekturen der Bürgerschaft obliegt es nun dem Ermessen der Behörden, ob sie Namen und Anschrift eines Auskunftsersuchenden weitergeben. Dabei müssen sie auch prüfen, ob nicht das Interesse des Antragstellers an der Geheimhaltung seiner Identität überwiegt. Appelle aus der Zivilgesellschaft oder von Caspar, mehr Transparenz für den öffentlich-rechtlichen Rundfunk in Norddeutschland zu schaffen oder die Ausnahme des gesamten Komplexes des Verfassungsschutzes von den Gesetzespflichten zu streichen, griffen der Senat und die Bürgerschaft nicht auf. Zudem entfällt die Anforderung an die Behörden, die begehrten Informationen „unverzüglich“ zugänglich zu machen. Es greift so nur noch die allgemeine Frist von einem Monat. Sollten Dritte angehört werden müssen, besteht künftig wegen des damit verbundenen „erhöhten Zeitbedarfs“ eine Verlängerungsoption von drei Monaten.

Dazu kommt erstmals eine Ausnahme von der Informationspflicht, soweit und solange dieser etwa der Patent- oder Urheberrechtsschutz entgegenstehen. Die veröffentlichungspflichtige Stelle muss beim Beschaffen einschlägiger Informationen aber zumindest darauf hinwirken, „dass ihr die erforderlichen Nutzungsrechte eingeräumt werden“. Andererseits wird von Anfang 2021 an auch die mittelbare Staatsverwaltung, zu der etwa die Handelskammer oder die öffentlichen Hochschulen gehören, wichtige Informationen von öffentlichem Belang verpflichtend in das Transparenzportal einstellen müssen. Gerichte hatten diese Bereiche öffentlichen Rechts nach Klagen u.a. des Chaos Computer Clubs (CCC) bislang außen vor gelassen. Die Parlamentarier forderten

zudem den Senat auf, das Transparenzportal übersichtlicher zu gestalten und die Bürger mit einer öffentlichen Kampagne noch stärker auf das Angebot aufmerksam zu machen.

Caspar begrüßte bei der Präsentation seines Tätigkeitsberichts Informationsfreiheit für 2018/19, dass Bürger mittlerweile „in erheblichem Maße“ ihre Rechte auf Akteneinsicht nutzten und „die Ablehnung von Anträgen auf Veröffentlichung oder auf Auskunftserteilung nicht mehr einfach hinnehmen“. Sie riefen immer öfter die Verwaltungsgerichte an, was zu einer größeren Rechtssicherheit führe. Die Richter schlügen dabei teils „Breschen in das Ablehnungsdickicht“. Insgesamt sei der Einsatz für mehr Transparenz in der Verwaltung, der demokratisch-rechtsstaatliche Prozesse beflügele, „ein erfolgreicher, aber auch sehr steiniger Weg“ (Krempl, Hamburg: Bürgerschaft verschlimmbessert Transparenzgesetz, www.heise.de 23.12.2019, Kurzlink: https://heise.de/-4623118)

Hessen

Mit aktivAPP und reha score gegen Arbeitslosigkeit

Die Kommunalen Jobcenter der Kreise Offenbach und Main-Taunus sowie der Stadt Offenbach wollen künftig Hartz-IV-Empfängern helfen, erwerbsfähig zu bleiben und starten gemeinsam ab Januar 2020 das Pilotprojekt „Kooperation für Prävention, Fitness und Gesundheit im Jobcenter“ (KOPF22). Das Projekt soll nach Angaben der Sozialdezernenten Carsten Müller (Kreis Offenbach), Sabine Groß (Stadt Offenbach) sowie Johannes Baron (Main Taunus-Kreis) dazu beitragen, die Gefahr, dass eine Person ihre Erwerbsfähigkeit mittel- oder langfristig verliert, besser abzuschätzen und zu reduzieren. Im Mittelpunkt stehen Männer und Frauen mit einem beginnenden Handicap und Menschen mit gesundheitlichen Einschränkungen. Carsten Müller: „Für sie sollen neue Beschäftigungschancen eröffnet werden, indem die Jobcenter neue Ansätze zur Unterstützung und zum Erhalt der Erwerbsfähigkeit über einen längeren Zeitraum erproben und auswerten.“

Ein zentraler Bestandteil des Projektes ist die Entwicklung einer „aktivAPP“. Mit ihr erfassen Langzeitarbeitslose persönliche Daten zu ihren individuellen Lebensbedingungen, woraus die App einen Wert berechnet; den sogenannten „reha score“. Dieser Score soll angeben, ob und wie stark die Erwerbsfähigkeit eines Menschen bereits gefährdet ist. Aus den Ergebnissen werden maßgeschneiderte Förderstrategien abgeleitet, um die Arbeitsfähigkeit des Einzelnen zu erhalten und zu stärken. Die jeweiligen Daten, aus denen sich der „reha score“ berechnet, bleiben, so die Mitteilung „anonym“.

Die Kooperation der Jobcenter mit Akteuren aus dem Bereich der medizinischen und beruflichen Rehabilitation soll zudem verbessert und die Zahl der Betroffenen, die eine Erwerbsminderungsrente, Eingliederungshilfen oder Sozialhilfe beziehen, nachhaltig gesenkt werden. Dabei gelte es, vor allem die Gesundheit sowie die körperliche Fitness des Einzelnen entscheidend zu verbessern, aber auch Menschen aus einem „mentalen Loch“ zu holen, unterstreichen die Sozialdezernenten. Dafür arbeiten die drei beteiligten Jobcenter bei dem Gemeinschaftsprojekt KOPF22 eng mit Ärzten und anderen Experten aus dem Gesundheitssystem zusammen. Das Projekt forciere damit auch eine engere Verzahnung von Arbeitsmarkt und Gesundheitssystem.

KOPF22 ist eins von 61 Modellvorhaben im Rahmen des Bundesteilhabegesetzes, mit denen Jobcenter und Träger der gesetzlichen Rentenversicherung innovative Instrumente zur Stärkung der Rehabilitation entwickeln. Ab Januar 2020 wird das Projekt für die Dauer von vier Jahren durch das Bundesprogramm „Innovative Wege zur Teilhabe am Arbeitsleben“ (rehapro) gefördert. Sabine Groß: „Die gewonnenen Erkenntnisse und Erfahrungen sollen die Förderstruktur nachhaltig verbessern und so die Chancen von Langzeitarbeitslosen mit einem Handicap oder krankheitsbedingten Einschränkungen auf einen sozialversicherungspflichtigen Job und gesellschaftlichen Teilhabe erhöhen.“ Zur Umsetzung des Bundesprogramms „rehapro“ stehen bis 2026 insgesamt rund eine Milliarde Euro zur Verfügung. Die einzelnen Modellprojekte können bis zu fünf Jahre gefördert werden (Erwerbsfähigkeit erhalten: Pro Arbeit und die Jobcenter der Stadt Offenbach sowie des Main-Taunus-Kreises starten Pilotprojekt, www.kreis-offenbach.de 13.12.2019).

Niedersachsen

Umstrittenes Polizeigesetz muss nachgebessert werden

Der Niedersächsiche Landtag musste sich in seiner letzten Plenarsitzung vor Weihnachten 2019 mit dem nach langem Tauziehen erst im Mai 2019 beschlossenen Polizeigesetz befassen. Wegen eines Urteils des Bundesverfassungsgerichts müssen Passagen im Gesetz zur automatischen Kennzeichenerfassung und zur Schleierfahndung nachgebessert werden (DANA 2/2019, 108 ff.). In dem Bundesland war über das Gesetz lange und kontrovers diskutiert worden (DANA 1/2018, 26 ff., 4/2018, 200 f.). Zwar gab es an der Notwendigkeit einer Gesetzesreform keine grundsätzlichen Zweifel. Völlig umstritten war jedoch, wie weit Behörden in die Privatsphäre von Bürgern eingreifen dürfen. Eine zunächst von Rot-Grün vorbereitete Gesetzesnovelle war nach einer völligen Überarbeitung von der SPD/CDU-Mehrheit beschlossen worden (DANA 3/2019, 155).

Die Polizei war zwischenzeitlich mit der Einführung von Körperkameras für Streifenbeamte oder mit Streckenradars gegen Raser vorgeprescht. Mit dem Gesetz gibt es dafür nun rechtliche Grundlagen. Das bei Hannover installierte bundesweit erste Pilotprojekt zur „Section Control“ musste auf eine Klage hin zunächst außer Betrieb genommen werden (DANA 2/2019, 110). Erst nach Verabschiedung des Gesetzes gab es grünes Licht vom Gericht. Und die Bodycams, die Beamte in potenziellen Konfliktlagen einschalten können, durften zunächst nur Bilder und keinen Ton aufnehmen, sind aber nun mit dem neuen Gesetz voll in Betrieb.

Die Landesdatenschutzbeauftragte Barbara Thiel lobte zwar so manche Nachbesserung im Gesetzesverfahren und das Beseitigen von aus ihrer Sicht

verfassungswidrigen Praktiken bei der Polizei. Doch kritisiert sie weiterhin den Betrieb der polizeilichen Telekommunikationsüberwachung (TKÜ). Die Eingriffsschwelle für viele polizeiliche Maßnahmen sei ohne stichhaltige Begründung herabgesetzt worden. Schon im Vorfeld einer konkreten Gefahrenlage könne die Polizei zu einer Online-Durchsuchung oder einer elektronischen Fußfessel greifen.

Nach wie vor wirft die Opposition der Regierung vor, ein nicht auf seine Verfassungsmäßigkeit überprüftes Gesetz beschlossen zu haben. Die mehrfache Ankündigung, den Staatsgerichtshof mit einer Prüfung zu beauftragen, scheiterte am Unwillen von FDP und Grünen, einen gemeinsamen Antrag mit der AfD einzureichen. Die beiden Parteien alleine kommen nicht auf die erforderliche Mindestanzahl von 20% der Abgeordneten. Die Parlamentarier von SPD und CDU lehnten es ab, das selbst beschlossene Gesetz in Frage zu stellen. Die von der AfD inzwischen alleine eingereichte Verfassungsklage wird mangels Unterstützung der anderen Parteien erfolglos bleiben.

Auch die Sicherheitsbehörden, deren Arbeit das neue Gesetz erleichtern soll, sind nicht zufrieden. Der Leiter der für Extremismusbekämpfung zuständigen Generalstaatsanwaltschaft Celle, Frank Lüttig, forderte den Abbau formaler und technischer Hürden bei der Online-Durchsuchung. Trotz der mit dem Polizeigesetz geschaffenen Möglichkeiten dazu seien Fahnder in der Praxis weiter auf ausländische Nachrichtendienste und deren Einsatz von Trojanern angewiesen: „Wir haben die Online-Durchsuchung im Gesetz, aber die Hürden sind zu hoch. Da sich alles im virtuellen Raum abspielt, brauchen wir funktionsfähige Online-Infiltrationsmöglichkeiten.“ Das Landeskriminalamt forderte, dass Telekommunikationsanbieter verpflichtet werden können, Inhalte unverschlüsselt zu übermitteln. Standortinformationen von Handynutzern müssten durchgängig verfügbar sein. Provider müssten zudem zur Mitwirkung bei polizeilichen Maßnahmen verpflichtet werden, so eine Sprecherin: „Dieser Regelungsbedarf wird als erforderlich angesehen, um mittels Telekommunikationsüberwachungen auch zukünftig entsprechend schwerwiegenden Gefahren begegnen und schwerste Straftaten verfolgen zu können“ (Evers, Niedersachsen: Umstrittenes Polizeigesetz muss angepasst werden, www.heise.de 08.12.2019, Kurzlink: https://heise.de/-4608113).

Rheinland-Pfalz

DSGVO-Bußgeld in Höhe von 105.000 € gegen Krankenhaus

Der rheinland-pfälzische Datenschutzbeauftragte Dieter Kugelmann teilte am 02.12.2019 mit, dass ein von ihm gegen ein Krankenhaus verhängtes Bußgeld in Höhe von 105.000 Euro wegen mehrerer Verstöße gegen die Datenschutz-Grundverordnung (DSGVO) von diesem akzeptiert worden sei. Die Datenschutzverletzungen seien nach einer „Patientenverwechslung bei der Aufnahme“ offenbar geworden. Daraufhin habe das Krankenhaus auch eine falsche Rechnung ausgestellt, was „strukturelle technische und organisatorische Defizite beim Patientenmanagement“ offenbart habe. Kugelmann begrüßte zugleich die Bemühungen des Krankenhauses, sein Datenschutzmanagement fortzuentwickeln und zu verbessern: „Mir kommt es darauf an, dass mit Blick auf die besondere Sensibilität der Daten beim Gesundheitsdatenschutz substanzielle Fortschritte erzielt werden“. Er wolle mit der Geldbuße ein Signal senden, „dass die Datenschutzaufsichtsbehörden auf dem Feld des Umgangs mit Daten im Gesundheitswesen besondere Wachsamkeit an den Tag legen“ (Krempl, DSGVO-Verstoß: Krankenhaus in Rheinland-Pfalz muss 105.000 Euro zahlen, www.heise.de 04.12.2019, Kurzlink: https://heise.de/-4604348).

Thüringen

Datenschutz-Hausdurchsuchung bei Drohnenpiloten

Polizeibeamte haben auf Veranlassung des Landesdatenschutzbeauftragten von Thüringen Lutz Hasse die Wohnung eines Drohnenbesitzers durchsucht. Bei der Aktion am 12.11.2019 wurden Datenträger beschlagnahmt. Hasse erklärte, es habe „akuter Handlungsbedarf“ bestanden. Ein Nachbar des Drohnenbesitzers hatte sich beschwert, dass dieser in den Abendstunden immer wieder eine Drohne fliegen lasse. Laut dem Hinweisgeber habe der Pilot nicht permanent Sichtkontakt gehabt, was darauf schließen lasse, dass er das Fluggerät mit einem Videomonitor steuere. Da die Drohne auch über andere Gärten fliege und sie dabei in die Nähe von Schlafzimmerfenstern komme, hielt Hasse „eine massive Beeinträchtigung der Rechte und Freiheiten“ der Nachbarn für wahrscheinlich.

Der Datenschützer beantragte einen Durchsuchungsbeschluss beim zuständigen Amtsgericht in Erfurt, dem dieses stattgab. Die Ordnungshüter beschlagnahmten bei der Durchsuchung Speichermedien, auf denen sich der Aufsichtsbehörde zufolge „mutmaßlich Videoaufzeichnungen mit personenbeziehbaren Daten befinden“. Die Drohne selbst konnten die Beamten nicht beschlagnahmen. Hasse will die Datenträger auswerten lassen und dann entscheiden, ob der Drohnenflieger eine Ordnungswidrigkeit begangen hat, für die ein Bußgeld fällig wird. Die Datenschutz-Grundverordnung (DSGVO) sieht vor, dass solche Sanktionen „wirksam, verhältnismäßig und abschreckend“ sein sollen.

Der Datenschützer erklärte, dass die Entscheidung für die Hausdurchsuchung wegen des grundrechtlich garantierten Rechts auf Unverletzlichkeit der Wohnung nicht leichtgefallen sei. Der Gesetzgeber hat eine Hausdurchsuchung grundsätzlich auch für Ordnungswidrigkeitenverfahren vorgesehen. Das Gericht wäge in einem solchen Fall aber zwischen dem durch die Maßnahme beeinträchtigten Grundrecht und dem Verfolgungsinteresse des Staates ab. Im vorliegenden Fall hätten „konkrete Tatsachen zur Verletzung der Privatsphäre“ Betroffener vorgelegen, „die den Anfangsverdacht wesentlich überstiegen“ (Krempl, Datenschutz: Hausdurchsuchung bei Thüringer Drohnenpiloten, www.heise.de 14.11.2019, Kurzlink: https://heise.de/-4586491)

Datenschutznachrichten aus dem Ausland

Weltweit

Patienten-Bilddaten ungeschützt im Netz

Gemäß Medienberichten waren sensible medizinische Daten von weltweit mehreren Millionen Patientinnen und Patienten auf offen zugänglichen Servern im Netz gelandet. In Deutschland seien mehr als 13.000 Datensätze betroffen, in mehr als der Hälfte sind auch medizinische Bilder wie Brustkrebsscreenings, Wirbelsäulenbilder und Röntgenaufnahmen enthalten. Die Daten seien bis Mitte September 2019 zugänglich gewesen und stammten von mindestens fünf verschiedenen Serverstandorten. Der größte Teil der deutschen Datensätze entfalle auf Patienten aus dem Raum Ingolstadt und aus Kempen in Nordrhein-Westfalen.

Gemäß den Recherchen lagen die Bilder und andere Patientendaten, insgesamt ca. 16 Millionen Datensätze, aus rund 50 Ländern von Brasilien über die Türkei bis Indien auf ungesicherten Servern offen im Netz. Besonders betroffen seien Patienten aus den USA, wo gemäß dem Bericht „allein bei einem einzelnen Anbieter für radiologische Untersuchungen ... nach einer Auswertung von ProPublica mehr als eine Million Datensätze von Patienten“ vorlagen. Es habe sich nicht um ein einzelnes großes Datenleck gehandelt, sondern um eine Vielzahl von ungeschützten Servern. Der Experte für Informationssicherheit Dirk Schrader habe weltweit mehr als 2.300 Rechner gefunden, auf denen die Datensätze offen lagen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde von IT-Sicherheitsforschern darüber informiert und hat gemäß eigenen Angaben die betroffenen Einrichtungen davon in Kenntnis gesetzt. Es lägen keine Erkenntnisse vor, dass die Daten tatsächlich in krimineller Absicht abgeflossen sind.

Bei den Daten handelte es sich oft um Bilder, die von Magnetresonanztomographie-Untersuchungen stammen (MRT). Diese Bilder würden von den Geräten auf einen speziellen Server geschickt. Das System werde für die Bildarchivierung verwendet, ein „Picture Archiving and Communication System“ (PACS). Auch Röntgenaufnahmen und Bilder aus der Computertomographie landeten auf diesen Servern.

Der Bundesbeauftragte für Datenschutz Ulrich Kelber sprach von einem „verheerenden Eindruck“. Nach jetzigem Kenntnisstand seien in Deutschland zwei Krankenhäuser betroffen. Es müsse nun geklärt werden, ob möglicherweise auch Drittanbieter in der Verantwortung stehen. Es sei nicht ausgeschlossen, dass es hohe Bußgelder geben werde. Bundesgesundheitsminister Jens Spahn mahnte höchste Datenschutzvorkehrungen in der gesamten Branche an: „Wir müssen noch stärker alle im Gesundheitswesen dafür sensibilisieren, wie wichtig Datensicherheit ist.“ Dies gelte für jede einzelne Arztpraxis, jede Apotheke, jedes Krankenhaus und für Dienstleister. Dabei sei auch sicherzustellen, dass Server gesichert seien. Dies sei in diesem Fall offenkundig nicht so gewesen und müsse abgestellt werden.

Die Patientenbeauftragte der Bundesregierung Claudia Schmidtke hat Krankenhäuser und Arztpraxen zum besseren Schutz von Patientendaten aufgefordert. Der Skandal um ungesicherte Informationen über Patienten lege den Schluss nahe, dass Gesundheitsanbieter „minimale Standards bei der Absicherung ihrer Daten nicht eingehalten“ hätten. „Das darf nicht sein!“ Patienten hätten „ein Recht darauf, dass ihre Daten bestmöglich vor einem unrechtmäßigen Zugriff Fremder geschützt werden“. Nötig seien einheitliche Datenschutzstandards, verschärfte Haftungsregelungen und die Berücksichtigung von Patientenrechten bei der Digitalisierung von Versorgungsleistungen. Schmidtke forderte alle Akteure im Gesundheitswesen auf, „die Patientenrechte und die Patientensicherheit für das digitale Zeitalter fit zu machen“. Ohne das Vertrauen der Patienten werde es keine Digitalisierung im Gesundheitswesen geben. Dabei biete die Digitalisierung „immense Vorteile“ im Gesundheitssystem. So könne die Digitalisierung durch neue Erkenntnisse über Krankheiten oder durch individualisierte Behandlungsoptionen die Patientenversorgung verbessern.

Maria Klein-Schmeink, gesundheitspolitische Sprecherin der Bundestagsfraktion der Grünen, verlangte angesichts der Vorfälle, dass dem Schutz der sensiblen Gesundheitsdaten eine größere Aufmerksamkeit gewidmet werden müsse. „Datenschutz und Datensicherheit müssen in unserem Gesundheitswesen so selbstverständlich werden wie Händewaschen“, sagte sie. Die Fälle müssten jetzt genau aufgeklärt werden. „Wir müssen wissen, ob es sich um individuelle Fehler oder eine fehlerhafte Soft- oder Hardware handelt. Es muss geprüft werden, ob es bei der Zulassung und Überwachung solcher Medizinprodukte Lücken gibt, die solche Pannen ermöglichen.“ Notwendig sei außerdem, dass die Datenschutzbehörden besser ausgestattet würden, um schnell und vielleicht sogar präventiv auf solche Vorkommnisse reagieren zu können. „Gerade in den sogenannten Primärsystemen in Krankenhäusern liegt noch manches im Argen. Hier sind erhebliche Investitionen nötig. Bund und Länder müssen daher zügig die Investitionsfinanzierung für Krankenhäuser reformieren.“

Der SPD-Gesundheitspolitiker Karl Lauterbach forderte hohe Strafen bei Datenlecks in Krankenhäusern. Die Kliniken müssten ein zertifiziertes Datenschutzkonzept vorlegen. Der Linken-Gesundheitspolitiker Achim Kessler forderte Spahn auf, das Recht der Patienten „auf Schutz ihrer Daten ins Zentrum stellen, statt die Interessen der Digitalkonzerne durchzusetzen“.

Monika Buchalik, Vizepräsidentin der Landesärztekammer Hessen bezeichnete das publik gewordene, vermutliche Patientendatenleck als Skandal. Dieses sei eine Katastrophe, da es das Vertrauen in den Umgang mit hochsensiblen Patientendaten erschüttere. Zugleich mache es deutlich,

dass veraltete digitale Sicherungssysteme schleunigst abgelöst werden müssten bzw. vorhandene, gute digitale Sicherungssysteme auch richtig eingesetzt werden müssten, um die Datensicherheit zu gewährleisten. Buchalik forderte die Krankenkassen außerdem auf, auch die Kosten für die Sicherungssysteme zu übernehmen, die in Praxen und Kliniken durch die IT-Anbindung entstehen. Edgar Pinkowski, Präsident der Landesärztekammer Hessen und Vorsitzender des Ausschusses „Patientensicherheit" bei der Bundesärztekammer, betonte, dass die Digitalisierung des Gesundheitswesens und die damit einhergehende Frage der Datensicherheit und des Datenschutzes in der kommenden Dekade eine zentrale Frage der Patientensicherheit sein werde (Auf Servern lagerten Millionen Patientendaten offenbar ungeschützt, aerzteblatt.de 17.09.2019).

Weltweit

Datenschutzaufsichtsbehörden vereinbaren engere Kooperation

Die Internationale Datenschutzkonferenz (IDSK) Ende Oktober 2019 in Tirana hat eine Arbeitsgruppe (Policy Strategy Working Group) eingesetzt, die Vorgaben für den Erhalt der Privatsphäre weltweit stärker vereinheitlichen soll. Die Vertreter von rund 120 einschlägigen Aufsichtsämtern aus mehr als 80 Ländern haben sich beim Jahrestreffen darauf verständigt, künftig noch stärker zu kooperieren, globale Standards zu setzen und das Verhältnis zwischen dem Recht auf informationelle Selbstbestimmung und anderen Grundrechten besser auszuleuchten.

Der Bundesdatenschutzbeauftragte Ulrich Kelber begrüßte den Schritt: „Die Digitalisierung sorgt dafür, dass Daten mittlerweile weltweit miteinander verbunden und abrufbar sind. Daher muss auch der Datenschutz grenzübergreifend eine Garantie zur Wahrung der essenziellen Grundrechte darstellen." In Europa habe die Politik mit der Datenschutz-Grundverordnung (DSGVO) hierzu bereits einen ersten Schritt getan. Die IDSK gehe diesen Weg nun konsequent weiter. Die Konferenz strebt laut Kelber für die Zukunft eine festere Struktur an, um neben dem jährlichen Treffen eine ständige Zusammenarbeit ihrer Mitglieder zu erleichtern. Dies sei ein Grund dafür gewesen, die IDSK in „Global Privacy Assembly" umzubenennen. Strategisch habe sich die Versammlung bis 2021 als Schwerpunkte Künstliche Intelligenz (KI) und besondere datenschutzrechtliche Anforderungen für den Schutz von Minderjährigen gesetzt.

Das Gremium verabschiedete mehrere Entschließungen, u.a. eine „zur Bedeutung des Datenschutzes als Grundrecht". Darin appellieren die Kontrolleure an die Regierungen weltweit, die Sicherung der Privatheit als Menschenrecht anzuerkennen und in nationalen Gesetzen zu verankern. Darüber hinaus fordern sie Unternehmen auf, nachweisbar Verantwortung für den Datenschutz und weitere Grundrechte zu übernehmen. Eine weitere Entschließung befasst sich mit sozialen Medien und gewalthaltigen extremistischen Inhalten. Die IDSK drängt damit die Betreiber sozialer Netzwerke, ihre Dienste und die Daten ihrer Nutzer vor Missbrauch zu bewahren. Zugleich müssten sie die Verbreitung terroristischer und extremistischer Botschaften stoppen, ohne dabei die Meinungsfreiheit aus den Augen zu verlieren. Dies gelte auch für die parallel geforderten Bemühungen, einschlägige Propaganda und Gewaltaufrufe als solche zu identifizieren und dagegen vorzugehen.

Die Plattformen sollten die zuständigen Strafverfolgungsbehörden über solche Funde und die eingeleiteten Schritte, sie zu löschen, informieren, heißt es in der Resolution. Dabei müssten die Rechtsstaatlichkeit und die Menschenrechte eingehalten werden. Netzwerkanbieter sollen zudem klare Regeln aufstellen, welche Inhalte sie als terroristisch oder in anderer Hinsicht als rechtswidrig ansehen. Nutzenden müsse klar sein, welchen Content sie posten dürften. Die Aufsichtsbehörden geben auch Hinweise dazu, wie sich menschliche Fehler im Vorfeld oder im Umgang mit Datenpannen vermeiden lassen (Krempl, Aufsichtsbehörden: Globale Standards für Datenschutz und gegen Online-Hass, www.heise.de 26.10.2019; Kurzlink: https://heise.de/-4569825).

Weltweit

Tiktok zwischen Hype, Zensur- und Datenschutzvorwürfen

Die US-Regierung lässt die erfolgreiche chinesische App Tiktok auf eine mögliche Gefährdung der nationalen Sicherheit hin untersuchen. Zwei Jahre nach dem Verkauf des US-Start-ups Musical.ly, dem wegen Verletzung des Kinderdatenschutzes von der FTC ein Bußgeld von 5,7 Mio. US-Dollar auferlegt worden war (vgl. DANA 3/2019, 165), an die chinesische Firma Bytedance prüft eine Kommission für ausländische Investitionen in den USA die Übernahme. Dabei gehe es auch um die angebliche Weitergabe von Daten an Behörden in China. Bytedance hatte demnach bei der Übernahme zugesagt, Musical.ly separat von seinen chinesischen Apps weiter zu betreiben. Ein Jahr später wurde das amerikanische Angebot jedoch in den Dienst Tiktok integriert. Ein Bytedance-Sprecher erklärte, das Vertrauen der Nutzenden und Behörden in den Vereinigten Staaten habe für das Unternehmen oberste Priorität. Tiktok sende keine Nutzerdaten nach China.

Tiktok ist die erste App eines chinesischen Anbieters, die weltweit zum Erfolg geworden ist. Genutzt wird die Anwendung vor allem von Teenagern. Das Prinzip ist simpel: Man zeichnet mit dem Smartphone ein Video auf und lädt es hoch, maximal 15 Sekunden dürfen die Aufnahmen lang sein – verdichtetes Youtube also. Sobald man Tiktok startet, beginnt im Hintergrund künstliche Intelligenz zu arbeiten, schon nach wenigen Videos, die man zu sehen bekommen hat, hat die App die Interessen ausgewertet und blendet zielsicher nur noch für den Nutzer relevante Clips ein. Jugendliche verbringen so Stunden mit Tiktok, hangeln sich von einem Video zum nächsten.

Alleine in den USA soll Tiktok bereits etwa 110 Millionen Mal heruntergeladen worden sein (in China 500 Mio.). Die aktuelle Bewertung von Bytedance liegt – auch deshalb – seit der letzten Investorenrunde bei sagenhaften 78 Milliarden US-Dollar und ist damit das höchstbewertete Start-up weltweit. Einem

internen Dokument zufolge sind rund 800 Millionen Nutzende registriert, in Deutschland 5,5 Millionen mit rasant steigender Tendenz. Mit 711 Mio. Downloads weltweit liegt Tiktok 2019 vor Facebook (659 Mio.) und Instagram (423 Mio.). Es ist damit das erste sog. soziale Netzwerk, das Facebook (Weltweit 1,9 Mrd. aktive Nutzende) und Instagram (1 Mrd. Nutzende) ernsthaft Konkurrenz machen könnte. Tiktok wächst schneller als jedes andere Netzwerk und findet insbesondere bei Kindern Anklang.

Die jüngste Prüfung wurde von Beschwerden im amerikanischen Kongress ausgelöst. Der demokratische Senator Chuck Schumer und der Republikaner Tom Cotton hatten den US-Geheimdienstkoordinator (DNI) Ende Oktober 2019 zur Einleitung einer Untersuchung aufgefordert. Die Senatoren forderten, dass die Experten „eine Einschätzung der Gefährdung der nationalen Sicherheit durch Tiktok und andere Plattformen in chinesischer Hand in den USA" abgeben. Obwohl Tiktok nicht in China erhältlich sei, müsse Bytedance den chinesischen Gesetzen Folge leisten, inklusive der Unterstützung der Geheimdienste. Dies könne ein mögliches Einfalltor für chinesische Spionage sein, hieß es.

Tiktok war auch kritisiert worden, weil kaum Aufnahmen der Proteste in Hongkong zu sehen waren. Zunächst hatte die Plattform das millionenfach aufgerufene Video einer Nutzerin gelöscht, die die Verfolgung muslimischer Uiguren in China anprangerte – wegen einer Verletzung der Richtlinien. Anschließend entschuldigte sich Tiktok für den Schritt und teilte mit, der Clip sei aufgrund eines „menschlichen Fehlers" vorübergehend entfernt worden und schnell wieder verfügbar gewesen. Netzpolitik.org legte offen, dass Tiktok laut internen Dokumenten Videos von Nutzerinnen und Nutzern mit Behinderung sowie dicken oder queeren Menschen verstecken, also in ihrer Reichweite beschränken soll. In den Moderationsregeln der Plattform wird das demnach als Schutzmaßnahme deklariert: Man müsse annehmen, dass es sich um Leute handle, bei denen man „auf Basis ihrer physischen oder mentalen Verfassung" davon ausgehen müsse, dass sie zum Ziel von Mobbing würden. Mark Zuckerberg, der Chef des Konkurrenten Facebook, der auch Instagram betreibt, warf Tiktok daher Zensur vor, die in den USA zu spüren sei. Die Firma wies den Vorwurf zurück.

Offiziell soll Tiktok erst ab einem Alter von 13 Jahren genutzt werden. Doch Videos gucken kann man auch ohne Anmeldung und Altersangabe. Laut einer Umfrage nutzt in Deutschland ein Viertel der 10- bis 13-Jährigen die App. Die App verlangt zwar keine Anmeldung. Anonym ist man dort dennoch nicht unterwegs: Auf fast jedem Smartphone gibt es Identifikationsnummern, die von den Apps ausgelesen werden. Meist sind es die Werbe-IDs von Google oder Apple. So wird der unangemeldete Nutzer zu einer Nummer, Tiktok enthält zudem die Software anderer Unternehmen, die auf die Analyse von Nutzerverhalten im Netz spezialisiert sind: Facebook und Appsflyer. Diese Firmen erhalten ständig Daten von der App: etwa Start und Ende der Nutzung, jedes angeschaute Video, die abonnierten Kanäle. In Tiktok eingegebene Suchbegriffe landen mit der Werbe-ID bei Facebook und können einem Facebook-Nutzer zugeordnet werden. Aus diesen zentral angereicherten Daten aller genutzten Apps kann man über die Zeit statistische Vorhersagen erstellen: Wohlstand, Lieblingsschuhmarke, politische Gesinnung.

Der juristische Datenschutz-Experte Malte Engeler bezweifelt die Rechtmäßigkeit des Angebots in Europa: Zum einen fehle bisher die nötige Transparenz, um zu erkennen, an wen die Daten nach der Weitergabe an Appsflyer gehen. Bytedance erklärte, dass die Datenweitergabe in den Datenschutzbestimmungen erläutert sei, aber über vertragliche Details keine Auskunft gegeben werden könne. Noch schwerer wiegt für Engeler aber die Übertragung der Nutzerdaten ins Ausland. Der Standort der Server, auf denen die Daten lagern (Japan und USA) sei zweitrangig. Entscheidend sei, wo der Sitz der Firma ist, die tatsächlich über die Daten bestimmt. Appsflyer sitzt nahe Tel Aviv, Bytedance in Peking: „In China muss man mit dem unbeschränktem und anlasslosen Zugriff der Behörden auf die Daten rechnen. Damit ist der Wesensgehalt des Grundrechts auf Achtung des Privatlebens verletzt."

Die Analyse der Datenströme zeigt, dass Tiktok in seiner Logik kein Überwachungsnetzwerk aus dem kommunistischen Politbüro ist, sondern einem sehr westlichen, kapitalistischen Konzept folgt. Kritiker nennen das Geschäftsmodell „People Farming": Leute werden mit psychologischen Tricks möglichst lang auf einer Plattform gehalten und schauen Inhalte, die sie im Idealfall selbst erstellt haben. Dann wird ihnen Werbung angezeigt, die anfallenden Daten über sie werden weitervermarktet. Dazu passt, dass Tiktok eine eigene Vermarktungsplattform gegründet hat (Giesen, Tiktok unter Verdacht, SZ 04.11.2019, 17; Eberl, Das Netzwerk, SZ 05.12.2019, 29; Böhm/Mingels/Rainer, Schwierige Pubertät, Der Spiegel Nr. 1, 28.12.2019, 70 ff.).

EU

Wiewiórowski neuer Europäischer Datenschutzbeauftragter

Wojciech Wiewiórowski ist am 26.11.2019 zum Datenschutzbeauftragten der EU-Institutionen gewählt worden. Der Ausschuss für Justiz und Bürgerrechte im EU-Parlament bestätigte mit breiter Mehrheit Wiewiórowski, der nach dem Tode seines Amtsvorgängers Giovanni Buttarelli (DANA 3/2019, 158) seit August dessen Aufgaben übernommen hatte. Der polnische Verfassungsrechtler soll zumindest bis Dezember 2023 Chef der europäischen Datenschutzbehörde bleiben. Der Europäische Datenschutzbeauftragte ist für die Einhaltung des Datenschutzes durch die EU-Institutionen zuständig und berät die EU-Kommission bei neuen Gesetzesvorschlägen. Die Behörde sitzt zudem im Europäischen Datenschutzausschuss, einem Gremium von Datenschützern aller EU-Staaten. Seit Wirksamwerden der Datenschutz-Grundverordnung (DSGVO) kommt der Behörde eine Schlüsselrolle bei deren Durchsetzung zu.

Der 48-jährige Wiewiórowski, in Brüssel auch als WW bekannt, galt unter Netzaktivisten und Datenschützern als stärkster Kandidat um das Amt. Gegen ihn traten der Franzose Yann Padova und der Ungar Endre Szabó an. Als gro-

ße Herausforderungen seiner Amtszeit nannte Wiewiórowski die Einführung von Künstlicher Intelligenz, Biometrie und automatisierte Gesichtserkennung, Blockchain und Quantencomputer. „Für alle diese Techniken können im Rahmen des Datenschutzes wichtige Leitlinien vorgegeben werden, und das sollte auch getan werden. Wenn wir unsere Standards senken, werden sich weltweit Länder zunehmend an anderen Modellen orientieren, etwa an jenem Chinas oder an jenen, die in den kommenden fünf Jahren in Indien und den Vereinigten Staaten entstehen werden."

Wiewiórowski kontrolliert künftig auch die Arbeit von EU-Einrichtungen wie der Polizeiagentur Europol und der Grenzbehörde Frontex. Bei der seiner Wahl vorausgegangenen Anhörung im EU-Parlament hatten einige Abgeordnete Wiewiórowski den Rücken gestärkt. Es sei klar, dass er einige „Überzeugungen und Sichtweisen" mit ihr teile, sagte die niederländische Abgeordnete Sophie in't Veld, die sich seit Jahren für digitale Rechte stark macht. Der EU-Abgeordnete der Piratenpartei Patrick Breyer meinte, neben seiner langjährigen einschlägigen Erfahrung zeichne ihn „seine Unabhängigkeit von Regierungs- und Industrieinteressen und seine Kontakte zur Bürgerrechtsbewegung" aus. Wiewiórowski hatte kurz vor seiner Wahl Anfang November in Brüssel die auch von vielen Aktivisten besuchte Digitalkonferenz „Freedom not Fear" eröffnet.

Der 1971 Geborene begann zur Zeit der Wende in seiner Heimat Polen sein Rechtsstudium. Vor seiner Anhörung schrieb er: „Ich bin in einem undemokratischen Land in einer Zeit großer Umbrüche aufgewachsen. Ich werde nie vergessen, welche Auswirkungen ein Überwachungsstaat und das Kriegsrecht auf ganz normale Menschen haben: das schreckliche Gefühl, wenn man weiß, dass die Behörden die Privatkorrespondenz und Telefongespräche routinemäßig kontrollieren, und zwar im Namen der ´Sicherheit` und zum ´Wohl der Allgemeinheit`. Ich schätze die Freiheit und Würde des Einzelnen aufgrund meiner eigenen Erfahrungen, und mir ist bewusst, wie wertvoll und zerbrechlich sie sind."

Nach seinem Studium arbeitete Wiewiórowski an der Universität Danzig und für das polnische Innenministerium zu IT-Recht. Ab 2010 leitete er Polens Datenschutzbehörde und arbeitete in EU-Datenschutzgremien mit, ab Dezember 2014 war er stellvertretender Europäischer Datenschutzbeauftragter. Mit dem Tod von Giovanni Buttarelli hatte Wiewiórowski das Amt des Europäischen Datenschutzbeauftragten vorübergehend übernommen. Nun erhielt er ein Mandat für die volle Amtszeit von fünf Jahren (Fanta, EU-Parlament bestätigt Europäischen Datenschutzbeauftragten, netzpolitik.org 26.11.2019; Datenschützer für EU, SZ 27.11.2019, 16).

Deutschland/Frankreich/Großbritannien

Psychowebseiten übertragen Nutzungsdaten für Werbezwecke

Eine Analyse von Privacy International (PI) zeigt, dass ein Großteil beliebter Webseiten, auf denen sich Besucher über psychische Krankheiten informieren können, Nutzungsdaten an andere Unternehmen weiterleitet, die augenscheinlich gar nichts mit den Gesundheits-Webseiten zu tun haben. Menschen, die unter Depressionen leiden und im Internet Hilfe suchen, genießen so keine Vertraulichkeit. Unter den beobachtenden Unternehmen sind große Werbenetzwerke sowie Google, Amazon und Facebook. Drittanbieter könnten anhand der weitergegebenen Daten erkennen, dass sich ein Besucher über psychische Erkrankungen informiert hat oder gar einen Depressions-Selbsttest gemacht hat. In vielen Fällen werden die Daten ohne die Zustimmung der Nutzenden weitergegeben.

Es gibt wenige Themen, die so schambesetzt sind wie psychische Krankheiten. Daten, die Rückschlüsse auf die Gesundheit Einzelner zulassen können, sollten deshalb nicht nur in den Krankenakten von Ärzten oder Psychologen besonders geschützt sein, sondern auch im Netz. PI, eine in London ansässige Datenschutzorganisation, untersuchte 136 viel frequentierte Webseiten für psychische Gesundheit in Deutschland, Frankreich und Großbritannien. Webseiten bestehen aus verschiedenen Software-Bausteinen. Nicht über alle davon hat der Betreiber der Seite die volle Kontrolle. Mehr als 97% der untersuchten Seiten enthielten Elemente von Drittanbietern. Diese können harmlos sein und zum Beispiel nur visuelle Effekte auf der Seite steuern. Andere werden aber eingesetzt, um den Besuchenden Werbung anzuzeigen, Daten über ihr Verhalten zu erfassen und an andere Firmen weiterzuleiten.

Die 44 untersuchten deutschen Seiten enthielten im Schnitt mehr als acht Elemente von Drittanbietern und übermittelten in mehr als sieben Fällen Tracking-Cookies solcher Firmen. Cookies sind Daten, die auf dem Gerät eines Internetnutzers gespeichert werden, wenn er eine Webseite besucht. Anhand einer eindeutigen Identifizierungsnummer können Cookies von Drittanbietern Nutzende über verschiedene Webseiten hinweg verfolgen. Ziel ist, ihnen passgenau maßgeschneiderte Werbung anhand der vermuteten Interessen anzuzeigen.

Fast zwei Drittel der von PI entdeckten Elemente wurden von den Gesundheits-Webseiten für Werbung eingesetzt. Die Seiten ermöglichen es Werbenetzwerken, ihre ohnehin große Datensammlung um intime Details zu ergänzen. Vier von neun näher untersuchten Seiten fragten der Studie zufolge nicht um Erlaubnis, bevor sie einen Cookie bei den Besuchenden hinterlegen. Ulrich Kühn, stellvertretender Leiter der Hamburger Datenschutzaufsichtsbehörde, erklärte, dass es ohne Einwilligung „keine Rechtsgrundlage" für die Datenweitergabe gebe. Das sei „ein klarer Verstoß gegen die Datenschutz-Grundverordnung" (DSGVO). Die DSGVO stellt Gesundheitsdaten auf eine Stufe mit Informationen über sexuelle Orientierung, genetische und biometrische Merkmale sowie Informationen über „rassische und ethnische Herkunft", Religion und Weltanschauung.

PI empfiehlt, dass Seiten, die sensible Themen wie psychische Gesundheit behandeln, komplett auf verhaltensorientierte Anzeigen verzichten. Die Organisation nahm auch Webseiten unter die Lupe, die Depressions-Selbsttests anbieten. In diesen Fällen wird auch die Adresse der Webseite an Werbetreibende weitergeleitet, wie etwa netdoktor.

de/selbsttests/depressionstest-nach-goldberg oder nie-mehr-depressiv.de/depressionstest/. Anhand der Adresse könnten Werbetreibende den Inhalt der Webseite herausfinden und ihn Besuchenden zuordnen. Dies dürfte vielen Hilfesuchenden sicher nicht gefallen. Einige Selbsttests erwecken den Eindruck, man könne sie komplett anonym nutzen, ohne dass dies zutrifft: Um die untersuchten Tests herum identifizierte PI jeweils Dutzende Tracker, die Informationen speichern und diese wiederum mit Informationen anderer Webseiten verknüpfen können. Dadurch können personenbezogene Profile entstehen.

Die Antworten der Selbsttests werden immerhin in den untersuchten deutschen Fällen nicht übertragen. Die Drittanbieter wissen im Zweifel nur, dass ein Nutzer einen Depressionstest gemacht hat und bis zu welcher Frage geklickt wurde. Für welche Antwortmöglichkeit sich der Nutzer entschieden hat, welche Symptome er also bei sich selbst beobachtet, kann aus den übertragenen Daten nicht geschlossen werden. Allerdings teilen mehrere französisch- und englischsprachige Webseiten die Antworten der Nutzenden mit Drittanbietern, wie PI in der Analyse schreibt.

Die Webseite Netdoktor.de ist eine der beliebtesten digitalen Anlaufstellen für Gesundheitsfragen in Deutschland. Gemäß PI setzt sie die meisten Drittanbieter-Elemente aller untersuchten deutschen Webseiten ein. Darunter ist etwa ein Cookie der französischen Werbefirma Criteo, die eigenen Angaben zufolge Daten zum Besucherverhalten auf mehreren Webseiten sammelt, um „relevantere" Werbung zu präsentieren. Laut PI hat ein Drittanbieter wie Criteo dadurch auch Zugriff auf die Adresse der Webseite und damit auf die Information, dass die BesucherIn einen Test aufgerufen hat. Netdoktor erklärt, dass keine Speicherung gesundheitsbezogener Daten stattfinde. Genauso wenig würden entsprechende Daten an Dritte weitergegeben oder gar veräußert. Man halte sich an geltendes Datenschutzrecht.

Allerdings kann beim Besuch der Webseite die IP-Adresse der Nutzenden und der Inhalt seitenübergreifender Cookies an eine Vielzahl von Drittanbietern übermittelt werden. Die IP-Adresse ist personenbeziehbar. In Kombination mit anderen Daten wie besuchten Webseiten ist sie besonders wertvoll für Werber. Frederike Kaltheuner von PI sagt: „Das Problem bei diesen Webseiten ist, dass schon die Adresse der Webseite sehr viel über uns preisgibt: Test, Symptome, bin ich depressiv – das sagt schon sehr viel über mich aus."

Auch die Internetseiten mehrerer deutscher Kliniken gehen laut der Untersuchung nicht sensibel genug mit den Daten ihrer Besucher um. Nach entsprechenden Anfragen der Presse erklärten mehrere der Kliniken, einzelne Marketing-Werkzeuge von Drittanbietern auf ihren Webseiten vorerst abzuschalten. Kurz vor der PI-Veröffentlichung hatte eine Recherche der Süddeutschen Zeitung gezeigt, wie problematisch Nachlässigkeit beim Umgang mit Informationen über die Gesundheit von Menschen im Internet sein kann. Die Webseite des Blutspendedienstes des Bayerischen Roten Kreuzes bietet eine Umfrage für potentielle Blutspender an, in der unter anderem nach HIV- und Hepatitis-Infektionen oder Schwangerschaftsabbrüchen gefragt wurde. Durch eine Fehlkonfiguration übertrug die Webseite wochenlang die Antworten an Facebook. Der Blutspendedienst hat diese Übertragung dann abgestellt. Das Bayerische Landesamt für Datenschutzaufsicht untersucht diesen Fall (Felix Brühl/Ebert/Eckert/Strozyk/Wormer, Depression: Wie Hilfesuchende im Netz erfasst werden, www.sueddeutsche.de 03.09.2019 = Überwacht beim Selbsttest, SZ 04.09.2019, 14).

Spanien

Volkszählung: Handytracking für statistische Zwecke

Für die im Jahr 2021 geplante Volkszählung will die spanische Statistikbehörde Instituto Nacional de Estadística (INE) Mobilitätsdaten von Millionen Bürgern erfassen. Dafür werden schon jetzt die Bewegungen von Mobilfunkgeräten in den Netzen der drei Anbieter Movistar (Telefónica), Vodafone und Orange getrackt. Kunden von Serviceprovidern (MVNO) sind nicht betroffen. Für die Analyse wurde an insgesamt acht Tagen erfasst, wie viele Handys sich zu bestimmten Uhrzeiten in bestimmten Abschnitten der Netze aufhalten. Die Behörde und die Netzbetreiber versichern, dass die Daten anonym gespeichert werden und keine Rückschlüsse auf die Identität der Handybesitzer erlauben. Die Daten werden von den Netzbetreibern aufbereitet und an die Behörde übermittelt. Spanischen Medienberichten zufolge erhalten die Unternehmen dafür insgesamt rund 500.000 €. Man werde von den Mobilfunkanbietern keine individuellen Informationen wie Telefonnummern oder Namen erhalten, betonte INE.

Im November 2019 fand die erste Phase der Datenerhebung statt, auch an einem Sonntag. Es folgte der erste Weihnachtsfeiertag. Als weitere Erhebungsperioden sind zwei Tage in den Sommerferien 2020 (20. Juli und 15. August 2020) geplant. Die Statistikbehörde möchte mit der Untersuchung im Rahmen der geplanten Volkszählung mehr Details über die Verhaltensweisen und Gewohnheiten der Bürger herausfinden: wo sie wohnen, wo und wann sie arbeiten, welche Verkehrsmittel sie benutzen, welche Wege die Verkehrsströme im Land nehmen und ob die Menschen an Weihnachten verreisen und wohin.

Eine Sprecherin der Verbraucherschutzorganisation OCU erklärte, eine solche Verwendung von Daten sei zu statistischen Zwecken „zwar grundsätzlich nicht illegal, auch wenn das ohne Einwilligung geschieht". Um sicher zu sein, ob wirklich alles anonym verläuft, „wäre es notwendig, den Vertrag zwischen dem INE und den Betreibern genauer zu untersuchen". Spanische Medien gaben unterdessen Tipps, wie die Spanier das Tracking ihrer Handys unterbinden können. Auch die Netzbetreiber reagierten teilweise. Vodafone bot seinen Kunden die Option, sich mittels der Kunden-App vom Tracking auszuschließen. Orange soll auf ihrer Website einen ähnlichen Service anbieten (Sperlich, Volkszählung: Behörde trackt Handys von Millionen Spaniern, www.heise.de 21.11.2019, Kurzlink: https://heise.de/-4594157).

Vatikan

Sexueller Missbrauch nicht mehr durch „päpstliches Geheimnis“ geschützt

Papst Franziskus hat am 04.12.2019 eine Regel für ungültig erklärt, durch die sexueller Missbrauch in der katholischen Kirche verschleiert wurde, und verschärft damit die Gangart beim Kampf gegen Missbrauch von Kindern in der katholischen Kirche. Dazu schaffte er das „päpstliche Geheimnis“ im Fall von Missbrauch durch Priester ab. Das „Päpstliche Geheimnis“ ist eine strenge Verschwiegenheitsregel in der katholischen Kirche. Das sogenannte Secretum pontificium stellt es unter Strafe, bestimmte Rechtsvorgänge öffentlich zu machen. Franziskus hatte festgestellt, dass diese Regel genutzt wurde, um Pädophile zu schützen, Opfer zum Schweigen zu bringen und die Strafverfolgungsbehörden davon abzuhalten, Verbrechen zu untersuchen.

Die Transparenzregel gilt für Beschwerden, Prozesse und Entscheidungen in Fällen sexueller Gewalt und ihren Vorstufen, wenn dies begangen wurde unter Androhung oder Missbrauch von kirchlicher Amtsautorität, wenn es um Missbrauch von Minderjährigen und Schutzbedürftigen geht, um Kinderpornografie sowie bei unterlassener Meldung oder Vertuschung von Missbrauch durch Bischöfe und Generalobere von Ordensinstituten. Es geht gemäß dem vatikanischen Mediendirektor Andrea Torinelli beispielsweise um Zeugenaussagen, die sich in Dokumenten befinden, die unter dem Päpstlichen Geheimnis in Archiven des Vatikans oder von Bistümern lagern. Diese können auch der weltlichen Justiz ausgeliefert werden. Aussagen in Kirchenprozessen können auch an zivile Behörden gehen. Informanten, Opfer und Zeugen können künftig bei kirchlichen Verfahren „nicht verpflichtet werden, zu den Fakten zu schweigen“.

Der massenhafte Missbrauch von Kindern hatte die katholische Kirche in eine ihrer schwersten Krisen gestürzt. Schon Franziskus‘ Vorgänger Benedikt XVI. hatte totale Transparenz angekündigt. Viele Kritiker sehen diese immer noch nicht durchgesetzt. Die deutschen Bistümer hatten ihre Zusammenarbeit mit den Staatsanwaltschaften seit 2010 intensiviert. Sobald sich ein Verdachtsfall sexuellen Missbrauchs erhärtet, soll er zur Anzeige gebracht werden.

Franziskus veröffentlichte insgesamt zwei Dokumente, sogenannte Reskripte, in denen er seine Autorität nutzt, um bestimmte Artikel des kanonischen Rechts neu zu schreiben. Mit diesen „Motu proprio“ wird unter anderem neu geregelt, in welchem Alter Minderjährige als Opfer von pornografischen Darstellungen gelten. Es gehört nun zu den schwersten Vergehen (graviora delicta), wenn solche Bilder mit Kindern im Alter von bis zu 18 Jahren verbreitet oder besessen werden. Bisher galt eine Grenze von 14 Jahren. Die Entscheidung des Papstes ist eine Folge des Antimissbrauchsgipfels im Vatikan im Februar 2019, zu dem Franziskus alle Bischöfe der Welt geladen hatte. Der Vorsitzende der Deutschen Bischofskonferenz Kardinal Reinhard Marx hatte sich dort für die Änderungen stark gemacht. Nach einer von der Bischofskonferenz veranlassten Studie missbrauchten allein in Deutschland zwischen 1946 und 2014 mindestens 1.670 katholische Geistliche 3.677 Minderjährige. Der Erzbischof von Malta und einer der engsten Papstberater beim Thema Missbrauch, Charles Scicluna, sprach von einer „epochalen“ Entscheidung.

Eine Hintertür bleibt jedoch auch nach dem Erlass: Die Verfahrensvorgänge unterliegen auch künftig einer besonderen Vertraulichkeit. Das Päpstliche Geheimnis wird nicht direkt abgeschafft, sondern eher herabgestuft auf die Ebene eines Amtsgeheimnisses. Das Amtsgeheimnis befreit nicht von Verpflichtungen durch staatliche Gesetze. Darunter fällt z.B. eine etwaige Meldepflicht bei Missbrauch. Eine solche Pflicht gibt es aber nicht überall, auch nicht in Deutschland. Generell umfasst das Päpstliche Geheimnis Geheimhaltungsnormen für bestimmte Rechts- und Verwaltungsakte der katholischen Kirche, etwa auch bei der Auswahl von Bischöfen. Zielsetzung ist der Schutz von Persönlichkeitsrechten. Magnus Lux von der Laienbewegung „Wir sind Kirche“ erklärte, die Entscheidung des Papstes habe große Tragweite, da Missbrauchsopfer bisher keinen Einblick hatten in kircheninterne Prozesse (Medichini, Franziskus schafft „päpstliches Geheimnis“ bei Missbrauch ab, www.spiegel.de 17.12.2019, Bachstein, „Päpstliches Geheimnis“ bei Missbrauch abgeschafft, SZ 18.12.2019, 1).

Russland

Deutsche Ermittlungen wegen Hacking

Der Hackerangriff auf die Welt-Doping-Agentur WADA im Jahr 2016 hat ein juristisches Nachspiel in Deutschland. Generalbundesanwalt Peter Frank hat in dem Zusammenhang ein Ermittlungsverfahren wegen „geheimdienstlicher Agententätigkeit“ eingeleitet. Hintergrund ist, dass bei dem Angriff vor drei Jahren auch die bei der WADA hinterlegten Daten deutscher Sportler, etwa des Tischtennisprofis Timo Boll oder der Speerwerferin Christina Obergföll, ausgespäht wurden. Die Ermittler schreiben den Angriff der Hackergruppe APT28 zu, auch bekannt unter „Fancy Bear“. Die Gruppe wird dem russischen Militärgeheimdienst GRU zugerechnet. Auf das Konto dieser Hacker sollen weltweit zahlreiche Angriffe auf hochrangige Ziele gehen. In Deutschland werden ihnen u.a. die Attacke auf den Deutschen Bundestag 2015, Angriffe auf politische Stiftungen und Medien vorgeworfen. Bei dem Angriff auf die WADA hatten die Hacker Daten über Dopingkontrollen zahlreicher Athletinnen und Athleten entwendet (Deutschland ermittelt gegen russische Hacker, Der Spiegel Nr. 47, 16.11.2019, 25).

Russland

Gesetzliche Internet-Totalkontrolle

Am 01.11.2019 wurde in Russland das „Souveräne-Internet-Gesetz“ in Kraft gesetzt, mit dem der Staat Zensur im und volle Kontrolle über das Internet realisieren möchte. Das Gesetz sieht eine umfangreiche Vorratsdatenspeicherung vor. Außerdem soll durch ein Gesetz ab Juli

2020 den Behörden und Geheimdiensten der Zugriff auf Daten von Smartphone- und Tabletnutzern erleichtert werden. Elektronische Geräte, die in Russland verkauft werden, müssen von da an mit Apps und Software russischer Unternehmen ausgestattet sein. Welche ausländischen Unternehmen betroffen sind und welche Apps vorinstalliert werden müssen, soll öffentlich gemacht werden, bevor das Gesetz ab Sommer 2020 in Kraft tritt. Doch schon jetzt wird gemutmaßt, wen es wohl treffen könnte – besonders heikel könnte es für Apple werden.

Vertreter des Apple-Konzerns sollen Presseberichten zufolge vor Umsetzung des Gesetzes damit gedroht haben, dass das Unternehmen den russischen Markt verlassen könnte. Die Installationspflicht würde das Geschäftsprinzip des Konzerns verletzen: Apple-Geräte werden grundsätzlich ohne vorinstallierte Apps und Browser von Drittanbietern verkauft. Russische Medien sprechen deswegen bereits vom „Anti-Apple-Gesetz".

Immer mehr ausländische Unternehmen werden zudem verpflichtet, die Daten russischer Nutzer auf russischen Servern zu speichern. Der Kreml argumentiert, damit wolle er russische Unternehmen stärken und Verbraucher vor Datenklau und Cyberangriffen aus dem Ausland schützen. Kritiker widersprechen: Es sei der Versuch, besser an die Daten von Millionen Russen zu kommen und deren Aktivitäten im Netz zu überwachen. Eine russische Wikipedia soll zudem aufgebaut werden, die, so Präsident Wladimir Putin, „verlässliche Informationen" bietet. Spätestens seit den Moskauer Massenprotesten von 2012 versucht die russische Regierung immer aggressiver, das Internet zu kontrollieren, blockiert Internetseiten und Apps.

Traditionell war in Russland das Fernsehen Informationsquelle Nummer Eins, doch die Sender werden mittlerweile staatlich kontrolliert. Daher informieren sich viele Russinnen und Russen lieber im Netz. Kritische Diskussionen finden auf Twitter statt. Über Facebook oder das russische Pendant VKontakte werden Demonstrationen organisiert, staatskritische TV-Formate sind inzwischen zu Youtube abgewandert. Auch der polarisierende Aktivist und Anwalt Alexej Nawalny veröffentlicht online Enthüllungsvideos – mit Millionen Klicks.

Menschenrechtler von Human Rights Watch kritisieren, das schwammig formulierte Souveräne-Internet-Gesetz erlaube alles – vom Blockieren einzelner Nachrichten bis zur kompletten Abschaltung des Internets. Tür und Tor werde geöffnet für eine Massenüberwachung, für politische Repression und eine Invasion in die Privatsphäre. Die russische Regierung begründet die mit dem Gesetz verbundene Abschottung auch damit, dass eine eigene Infrastruktur für ein souveränes Netz mögliche Cyberangriffe aus dem Ausland verhindern soll. Präsident Putin hatte das Gesetz im Mai 2019 unterzeichnet und die Kritik von Netzexperten und Menschenrechtlern zurückgewiesen. Egal, was es koste, die Rohstoff- und Atommacht müsse ein autonomes Internet haben. Das sei eine Frage der nationalen Sicherheit.

Der russische Internetexperte Alexander Isawnin von der unabhängigen Organisation Roskomswoboda (Für die Freiheit des Netzes) erklärte dagegen: „Damit übernimmt der Staat erstmals die volle technische Kontrolle über das Internet." Schon bisher war es so, dass viele Internetseiten, die etwa in Deutschland frei abrufbar sind, für russische Nutzende gesperrt blieben – etwa die des Regierungsgegners Michail Chodorkowski. Die Menschenrechtsorganisation Agora sieht das Gesetz als „fundamentale Wende" in der Regierungspolitik bei der Kontrolle des Internets. Tausende – vor allem junge Menschen – hatten im Frühjahr 2019 gegen das Gesetz demonstriert. Sie befürchten, der Kreml könnte künftig nach Belieben das Internet aus politischen Gründen abschalten.

Das wies Putins Sprecher, der im Kreml für Internetfragen zuständige Dmitri Peskow, als Unsinn zurück. Niemand habe die Absicht, Russland vom World Wide Web abzukoppeln. Vielmehr bestehe die Gefahr, dass der Westen Russland vom Netz abklemme. Deshalb brauche das Land eine unabhängige digitale Infrastruktur. Geschaffen werde nur eine Reservestruktur für mehr Sicherheit, behauptete der Chef des Ausschusses für Informationspolitik in der russischen Staatsduma Leonid Lewin. Das „Runet" bleibe ein Teil des weltweiten Netzes. Es gehe um einen sicheren Netzzugang für russische Nutzende unabhängig von der Arbeitsweise ausländischer Anbieter. Zudem solle das autonome Netz nur übungsweise oder im Fall von Gefahr von außen genutzt werden.

Der Internetaktivist Isawnin sieht auch wirtschaftliche Interessen hinter dem Gesetz. Ziel sei es, die Zahl der rund 5.000 Anbieter auf dem bisher freien Markt durch direkte staatliche Einmischung zu reduzieren. Technisch sei noch vieles ungeklärt. Klar sei aber, so Isawnin, dass der russische Internetverkehr künftig über Knotenpunkte im eigenen Land gelenkt werden solle. Die Infrastruktur dafür müsse erst noch aufgebaut werden. Zunächst sollen sich Provider Geräte anschaffen, die es der obersten Aufsichtsbehörde Roskomnadsor erlauben, direkt Inhalte zu kontrollieren und den Datenverkehr zu steuern. Der bisher freie Markt werde damit zerstört: „Mit dem Gesetz hat der Staat das Instrument, sich direkt einzumischen. So etwas gibt es bei Ihnen in Deutschland nicht. Und nach allen bisherigen Erfahrungen, ist jetzt das Schlimmste zu erwarten." Isawnin befürchtet, dass bei einer zunehmenden Monopolisierung das Internet künftig langsamer und teurer werden könnte. Insgesamt sei aber auch fraglich, ob das technisch alles überhaupt funktionieren könne.

Konzerne klagen schon jetzt über enorme Kosten, weil sie den Datenverkehr monatelang speichern müssen. Die Unternehmen forderten unlängst den russischen Staat auf, der die Gesetze erlasse, die Kosten dafür zu tragen. Der bisher freie Markt wird damit, so Isawnin, zerstört. Der russische Staat will die komplett neue Infrastruktur schaffen, um insbesondere von amerikanischen Konzernen, bei denen bisher der Großteil der Daten lagert, unabhängig zu sein. Die russische Regierung stört sich schon seit Langem daran, dass vor allem die westlichen Internetkonzerne Zugriff auf die wertvollen Datensätze haben. Die Daten russischer Bürger dürfen nach einem anderen Gesetz schon jetzt nicht mehr auf Servern im Ausland gespeichert werden. Das führte etwa zur Sperrung des Karrierenetzwerks LinkedIn in Russland.

Gegen Facebook und Twitter gab es bisher vor allem Drohungen und Ordnungsstrafen. Gesperrt sind die Zugän-

ge aber nicht. Die Organisation Reporter ohne Grenzen (ROG) sieht in dem Gesetz einen Angriff auf die Presse- und Meinungsfreiheit. Kontrolle und Filterung des Datenverkehrs lägen nun bei der Medienaufsicht und dem Geheimdienst. Deshalb sei das Gesetz eine Bedrohung für die Freiheit des Internets, der Versuch einer Zensur. ROG-Geschäftsführer Christian Mihr: „Es belegt, dass die russische Führung bereit ist, die gesamte Infrastruktur des Netzes unter politische Kontrolle zu bringen, um bei Bedarf den digitalen Informationsfluss abzuschneiden."

Schon während der Proteste im Sommer 2019 wurde ein Vorgeschmack darauf vermittelt, was künftig noch kommen könnte. Ein Absetzen von Nachrichten in sozialen Netzwerken oder auch nur Telefonieren waren teils nicht mehr möglich. Bei Protesten in der russischen Teilrepublik Inguschetien im Nordkaukasus 2018 wurde der Zugang zum Internet dortigen Medien zufolge einfach gesperrt.

Der Internet-Ombudsmann Dmitri Marinitschew erklärte: „Es braucht viel Anstrengung, um gegen die negativen Folgen des Gesetzes anzukämpfen." Noch seien die freiheitsliebenden Reflexe in der russischen Gesellschaft intakt – anders als etwa in China, wo das Internet nie frei gewesen sei: „Die ‚Daumenschrauben' lassen sich vielleicht kurzfristig fester ziehen, um irgendwelche lokalen Aufgaben zu erledigen, aber ein ‚chinesisches Internet' lässt sich schon nicht mehr umsetzen." Er äußerte die Hoffnung, dass das Gesetz am Ende wieder aufgehoben wird (Internet in Russland kommt unter staatliche Kontrolle, www.zeit.de 01.11.2019; Mauder, Russland schafft sich sein eigenes Internet, Kieler Nachrichten, 02.11.2019, 4; Lipkowski, Unter staatlicher Kontrolle, SZ 08.01.2020, 19).

USA u.a.

IT-Unternehmen greifen auf Gesundheitsdaten

Auf der weltgrößten Medizinmesse „Medica" in Düsseldorf im November 2019 waren die Themen Big Data, KI und selbstlernende Maschinen dominierend. Internetriesen wie Google, Facebook und Amazon wollen sich Patientenakten und Gesundheitsdaten sichern. NRW-Digitalminister Andreas Pinkwart betonte dagegen mehrfach: „Die Patienten müssen die Souveränität über ihre Daten behalten." Er verwies dabei auf europäische und deutsche Standards beim Datenschutz. Davon unbeeindruckt sind US-Internetgiganten wie Google, Facebook und Amazon dabei, sich auf dem Weg über spezialisierte Gesundheits-Websites bzw. direkte Verträge mit Klinikbetreibern den Zugang zu Millionen Patientenakten und hochsensiblen Gesundheitsdaten zu sichern. Google bestätigte, auf technischem Gebiet eng mit der großen amerikanischen Gesundheitskette Ascension zusammenzuarbeiten, die 2.600 Einrichtungen des Gesundheitssystems – von der Klinik bis zum Seniorenheim – verwaltet. Inzwischen soll das US-Gesundheitsministerium prüfen, inwieweit es bei dieser Auftragsdatenverarbeitung Verstöße gegeben hat.

Gemäß Presseberichten sollen seit 2018 Patientendatensätze von 51 Millionen Bürgern aus 21 Bundesstaaten weitergeleitet worden sein, ohne dass Patienten oder Ärzte davon wussten. Namen, Geburtsdaten, Laborergebnisse und Klinikdokumente landeten beim IT-Unternehmen. Mindestens 150 Mitarbeiter sollen einen Zugriff darauf haben – Arbeitstitel: „Project Nightingale" (Nachtigall). Mit der Datenflut will Google nach eigenen Angaben gemeinsam mit Ascension KI-Anwendungen und maschinelles Lernen testen. Experten sehen darin aber auch einen Ansatz Googles, in die milliardenschwere Gesundheitsbranche einzusteigen.

Ein weiterer Ansatz der Internet-Riesen, an Gesundheitsdaten zu gelangen, besteht darin über Internet-Aktivitäten auf Gesundheits-Websites Daten zu medizinischen Symptomen und Krankheitsbildern zu sammeln. Die Datenweiterleitung erfolgte in Großbritannien bei Stichwörtern wie Abtreibung oder Drogen – ohne Einverständnis der Internet-Nutzer. Davon profitiert u.a. DoubleClick, ein Google-Werbeunternehmen. In Deutschland hat der Ethikrat gefordert, dass bei KI-Einsatz und Big Data im Gesundheitsbereich die Datensouveränität im Vordergrund stehen muss. Patienten sollen mitbestimmen können, wie und in welchem Kontext ihre Daten verwendet und weitergeleitet werden (Kleideiter, Problem Datenschutz: Google & Co. haben Zugriff auf sensible Gesundheitsdaten, www.wn.de 24.11.2019).

USA

US-Regierung speichert DNA-Proben von Flüchtlingen

Die US-Regierung unter Donald Trump startete im Januar 2020 nach einer Gesetzesänderung die Erhebung von DNA-Proben von Asylsuchenden und anderen Einwanderern, die von Ausländerbehörden festgehalten werden. Gemäß einer Veröffentlichung des Innenministeriums (Homeland Security) geht der Schritt zurück auf „DNA Fingerprint Act" von 2005. Dieser besagt, dass die genetischen Informationen von jeder wegen einer möglichen Straftat gegen das Land festgenommenen Person gespeichert werden dürfen. Bisher zählte das Überschreiten der US-Grenze nicht dazu.

Für die Erhebung mittels eines Abstrichs aus der Wange zuständig sind sowohl die Grenzschutzbehörde (CBP) als auch der Zollschutz (ICE), jeweils zunächst in unterschiedlichen Grenzbereichen. Das FBI wertet die Daten aus und speichert sie in seiner Datenbank ab. Ausgenommen sind Kinder unter 14 Jahren, Senioren über 79 und Menschen mit psychischen oder physischen Einschränkungen. Erfasst wird, wer unzulässig einreist. Gemäß den Presseberichten laufen die neuen Regeln darauf hinaus, dass mit den Daten von hundertausenden Immigranten eine umfangreiche neue Datenbank aufgebaut wird. Kritiker halten die Maßnahme für verfassungswidrig.

Die USA sind dabei, ein riesiges Biometrie-Überwachungsnetz aufzubauen. Neben Homeland Security hat auch das Pentagon (Verteidigungsministerium) eine Datenbank, in der 7,4 Millionen Identitäten gespeichert sein sollen. In der „Next Generation Identification"-Datenbank (NIG) des FBI sollen 2016 bereits mehr als 411 Millionen Menschen

erfasst gewesen sein. Dort werden neben DNA-Daten auch Informationen zu Gesichtsbildern, Iris-Aufnahmen und Fingerabdrücke gespeichert. (Trump Administration to Change Rules to Allow it to Collect Asylum-Seekers´ DNA, Says Report, www.thedailybeast.com 21.10.2019; Weiß, USA sammeln DNA-Daten von illegalen Migranten, www.heise.de 07.01.2019, Kurzlink: https://heise.de/-4629636; vgl. DANA 4/2019, 230).

USA

Schulische Kommunikationsüberwachung zwecks Verhinderung unerwünschter Ereignisse

Der Dienstleister Gaggle überwacht die digitale Arbeit und Kommunikation von rund 5 Mio. SchülerInnen in den USA im Kampf gegen Selbstmorde und Amokläufe. Die Firma setzt auf einen Mix aus einem proprietären System mit Künstlicher Intelligenz (KI) und menschlichen Begutachtern von als schädlich oder gefährlich erkannten Inhalten, um potenziell tödliche Taten zu verhindern. Zugleich soll das Programm dabei helfen, Kinder und Jugendliche zu „guten Bürgern" zu erziehen. Mit dem Ansatz wirft die Firma aber Fragen nicht nur zum Datenschutz der Betroffenen auf.

Über 1.400 US-Schulen glauben bereits den Versprechen von Gaggle und setzen die Software ein, um die digitale Arbeit und Kommunikation ihrer Schutzbefohlenen „in Echtzeit" zu überwachen. Das Programm klinkt sich in Googles G Suite und Microsoft Office 365 und damit in zwei der am weitesten verbreiteten Produktivitätspakete in der Cloud ein und analysiert den gesamten damit erzeugten Datenverkehr. Es bezieht zudem Nachrichten aus Twitter, Facebook, Instagram und anderen sozialen Netzwerken mit ein, die mit einer schulisch benutzten E-Mail-Adresse verknüpft sind.

Gaggle behauptet, allein im Schuljahr 2018/19 722 Schüler von einem Suizid abgehalten zu haben. Interne Dokumente wie Hinweise für Prüfer von Inhalten, Fallberichte und Rechnungen aus 17 Schulbezirken, die das Online-Magazin BuzzFeed auf Basis des US-Informationsfreiheitsgesetzes erhalten und ausgewertet hat, zeigen, wie tief das System in die Privatsphäre der Betroffenen eingreift und dass die Erfolgsmeldungen auf nur schwer nachprüfbaren Kriterien beruhen. Zudem wird deutlich, dass Schulbezirke mehr als 60.000 US-$ für den Einsatz von Gaggle pro Jahr bezahlen, die in knappen Etats an anderer Stelle fehlen.

Die Software mit dem eingebauten KI-Filter scannt demnach E-Mails, Dokumente, Chats und Kalendereinträge und gleicht sie mit einer schwarzen Liste ab, auf der sich neben Ausdrücken mit Bezügen zu Selbstverletzungen, Gewalt, Mobbing oder Drogen auch „vulgäre Ausdrücke" befinden. Letztere machen dem Bericht zufolge 80% der von dem System zur weiteren Verfolgung markierten Inhalte aus. Auch Begriffe wie „schwul", „lesbisch" oder „queer" sind auf der Liste. Hinzu kommt ein „Anti-Pornografie-Scanner", über dessen Trainingsdaten Gaggle aufgrund der sensiblen Thematik und geschützter Informationen rund um die Eigenlösung keine Auskunft geben wollte. Stellt ein Analyst der Firma fest, dass ein Schüler pornografische Inhalte selbst erstellt hat, wird die Datei automatisch an das National Center for Missing and Exploited Children (NCMEC) weitergeleitet für einen weiteren Abgleich mit der dortigen Datenbank für Bilder mit sexuellen Missbrauchsdarstellungen von Kindern.

Schlägt die Software Alarm, übergibt sie einschlägiges Material an einen von 125 „Sicherheitsrepräsentanten 1. Grades". Erkennen auch diese darin eine immanente Bedrohung für Schülerinnen und Schüler, schaut noch ein Mitglied einer 25-köpfigen Kerngruppe von besonders geschulten Prüfern darüber. Bleibt es bei der Einschätzung, werden umgehend Zuständige bei der Ausbildungsstätte oder bei deren Nichterreichbarkeit bei der örtlichen Polizei informiert. Generell speist Gaggle Erkenntnisse aus der Kommunikationsüberwachung in ein „Dashboard" für das „Sicherheitsmanagement" ein, auf das auch Schuladministratoren Zugriff haben. Daraus ersichtlich werden „Regelverletzungen" einzelner Schülerinnen und Schüler zusammen mit deren Ausweisnummern. Die Betroffenen werden dabei in drei Risikogruppen eingeteilt, die von hohen bis zu niedrigen Bedenken mit nur „fragwürdigen Inhalten" reichen.

Das System befolgt auf dieser Basis eine „Three Strikes"-Regel, wie sie ähnlich auch aus dem Umgang mit Urheberrechtsverletzungen mit Konsequenzen bis hin zu Netzsperren bekannt geworden ist. Demnach werden auch geringfügige Regelverstöße an eine Schule gemeldet, wenn sie wiederholt auftreten und ein Beobachteter etwa dreimal das Wort „Fuck" benutzt. Betroffene verlieren damit gewisse Nutzerprivilegien, bis ein Schulvertreter sie wieder freischaltet.

Im jüngsten Schuljahr will das Unternehmen mithilfe des Programms 52.000 Hinweise auf Absichten für Selbstmorde und -verletzungen ausgemacht haben. Davon sollen 6.000 so dringlich gewesen sein, dass man die Schule unverzüglich darüber in Kenntnis gesetzt habe. Aus den Papieren geht aber hervor, dass die Software auch Dateien mit Titeln wie „Gedichtsammlung" oder „erzählerischer Aufsatz" als brandgefährlich eingeschätzt und so Fehlalarme ausgelöst hat. Gaggle „empfiehlt" Schulbezirken nach eigenem Bekunden, die Erlaubnis von Eltern und SchülerInnen einzuholen, bevor sie die Software der Firma verwenden. Sollten sich einzelne Betroffene später für ein Opt-out entscheiden, könnten sie die von der Schule angebotenen Softwareprodukte und E-Mail-Dienste nicht mehr in Anspruch nehmen und müssten mit eigenen Alternativen arbeiten. Von einer echten freiwilligen Nutzung des Dienstes lässt sich also nicht ausgehen.

Experten sehen den Einsatz des Systems kritisch. Sarah Igo, Geschichtsprofessorin an der Vanderbilt-Universität, erklärte, Schulen seien zwar schon immer „Trainingsstätten für die Persönlichkeit" gewesen. Unter der ständigen Aufsicht von Diensten wie Gaggle würde den Heranwachsenden auch vielleicht das ein oder andere beigebracht, „aber nicht das, was sie lernen sollen". Sarah Roberts, Expertin für „Content Moderation" an der University of California in Los Angeles, stellte fest, dass es sich hier offenbar um eine „Lösung auf der Suche nach einem Problem" handelt. Das Ganze funktioniere nur, „wenn wir

akzeptieren, dass unsere Kinder bis auf Weiteres in einem digitalen System gefangen sein sollten, schon letztlich von der Zeit an, in denen sie empfindungsfähig werden" (Krempl, Gaggle: Echtzeitüberwachung von US-Schülern mit Künstlicher Intelligenz, www.heise.de 02.11.2019; Kurzlink: https://heise.de/-4574230).

Vereinigte Arabische Emirate

Staatlicher Spionage-Messenger ToTok

Die New York Times berichtete unter Berufung auf nicht genannte US-Beamte und eine eigene Analyse, dass die sich zunehmender Beliebtheit erfreuende Chat-App namens ToTok ein Spionage-Werkzeug ist, das für die Regierung der Vereinigten Arabischen Emirate (VAE) entwickelt worden ist. ToTok ist gerade einmal ein paar Monate alt und wurde allein unter Android bereits mehr als fünf Millionen Mal heruntergeladen und installiert. Mit ihr können Nutzende Nachrichten austauschen, Fotos und Videos verschicken, ähnlich wie Whatsapp, Telegram oder Signal. Entwickelt wurde sie dem Bericht zufolge von einer Firma in den Emiraten, hinter der sich ein Dienstleister verbergen soll, bei dem unter anderem ehemalige US-Geheimdienstarbeiter für die Regierung des Golfstaats hacken.

Der Messenger sei ein clever entwickeltes Werkzeug zur Massenüberwachung: Standort, Kontakte, Mikrofon- und Kamerazugriff und weitere lokale Daten – alles steht zur freien Verfügung des VAE-Geheimdienstes. Für die Nutzer funktioniere die App wie eine der unzähligen Apps unter Android und iOS, die die Ortsdaten und Kontakte der Benutzer aufzeichnen. Im Gegenzug für den Zugriff auf den Standort verspreche die App einen passgenauen Wetterbericht und die Suche nach neuen Kontakten. Eine Ende-zu-Ende-Verschlüsselung wird nicht angeboten. Der Name spielt offenbar auf das beliebte chinesische soziale Netzwerk TikTok an. Statt also Hackern viel Geld für Werkzeuge oder Sicherheitslücken zum Zugriff auf Smartphones zu bezahlen, habe es die Regierung der Emirate geschafft, Millionen dazu zu bewegen, ihre Daten freiwillig herzugeben. Etwas versteckt habe es in den Angaben zu ToTok geheißen, dass „wir ihre persönlichen Daten mit Firmen der Gruppe teilen" könnten. Hinter ToToks Betreiberfirma Breej Holding steckt gemäß dem Bericht eine Hacking-Firma aus Abu Dhabi namens Dark Matter, die eine zentrale Rolle im digitalen Überwachungssystem der VAE spielt.

Laut New York Times werden in dem Golfstaat einige Funktionen von WhatsApp und Skype blockiert. Das habe zu dem schnellen Erfolg von ToTok beigetragen. In den Emiraten sei die App besonders beliebt gewesen, aber zuletzt auch in Saudi-Arabien, Großbritannien, Indien, Schweden und anderen Staaten. Sowohl auf Google Play als auch in Apples App-Store wurde die App von den Nutzern sehr positiv bewertet. Nach Anfragen der New York Times an Apple und Google wurde sie erst Dezember 2019 von beiden Anbietern gesperrt. Die Kontrollmechanismen der beiden Konzerne gegen bösartige Software hatten zuvor offenbar nicht funktioniert. Bereits über diese Stores installierte Apps funktionieren weiter.

ToTok reagierte auf die Sperrung in den beiden App-Stores und erklärte, „einige Nutzer" hätten berichtet, dass sie die App nicht herunterladen können. „Tatsächlich" sei die App wegen eines „technischen Problems" aktuell nicht überall verfügbar. Man arbeite mit Google und Apple an einer Behebung. In anderen App-Stores sei die Software aber weiterhin verfügbar und könne direkt heruntergeladen werden. Auf die erhobenen Vorwürfe gingen die Entwickler mit keinem Wort ein.

Hacker in den Diensten der Vereinigten Arabischen Emirate waren Anfang 2019 in den Fokus der Aufmerksamkeit gerückt. Damals hatte die Nachrichtenagentur Reuters öffentlich gemacht, dass Ex-Geheimdienstmitarbeiter aus den USA in Diensten des Golfstaats zahlreiche iPhones von Diplomaten, Politikern und Menschenrechtsaktivisten gehackt haben. Eine von ihnen erklärte damals, sie habe den Abschied von den Beschränkungen der NSA als berauschend empfunden: „Da gab es nicht diese schwachsinnige Bürokratie." Erst als sie entdeckt habe, dass auch US-Amerikaner ausspioniert wurden, sei das für sie zu weit gegangen. Nach ihren Protesten wurde sie entlassen (Holland, ToTok: Chat-App als Spionagewerkzeug für Vereinigte Arabische Emirate, www.heise.de 23.12.2019, Kurzlink: https://heise.de/-4622039, Muth, Geheimdienst im Handy, SZ 24.12.2019, 8).

Afrikanische Staaten

Zunehmend Datenschutzgesetze – nicht immer mit mehr Datenschutz

Wer es in Kenia mit dem Datenschutz nicht so genau nimmt, kann dafür künftig hinter Gittern landen. Zwei Jahre Haft oder bis zu 26.000 Euro Geldstrafe sieht das neue Datenschutzgesetz des Landes für diese Fälle vor, das seit Anfang November 2019 in Kraft ist. Informationsminister Joe Muchuru lobte das Gesetz, für das die Datenschutz-Grundverordnung (DGSVO) der Europäischen Union Vorbild sei: „Beim Datenschutz ist Kenia nun Teil der internationalen Gemeinschaft geworden".

Andere afrikanische Länder wollen nachziehen. Gambias Informationsminister Ebrima Sillah kündigte auf dem UN-Internetforum im November 2019 an: „In den nächsten 20, 30 Jahren wird es mehr Internetnutzer in Afrika geben als in Europa und Amerika zusammen. Wir machen uns große Sorgen, wer unsere Daten nutzt und wofür." Immer mehr Menschen nutzten mobile Geldtransfers wie Mpesa, buchten Flugtickets online, verschickten WhatsApp-Nachrichten. Dabei entstünden riesige Datenmengen, mit denen Internetfirmen machen können, was sie wollen.

Leishen Pillay, Datenschutz-Experte der Consultingfirma Deloitte in Südafrika, erklärte: „Es gibt in Afrika nur einige Inseln der Regulierung." Dies seien kleine Inseln: Weniger als die Hälfte der afrikanischen Länder haben Datenschutzgesetze. Einheitliche Standards wie die DGSVO in der Europäischen Union gibt es auf dem Kontinent nicht: „Das wäre die Wunderwaffe für den Datenschutz." 2014 beschloss die Afrikanische Union eine Datenschutz-Konvention. Die ist aber noch nicht in Kraft, weil sie bisher gerade mal von fünf Mitgliedsländern ratifiziert worden ist.

Cécile Barayre, Datenschutzexpertin bei der UN-Konferenz für Handel und Entwicklung (UNCTAD), wies zudem auf ein Vollzugsdefizit hin: „Wir sehen seit einigen Jahren eine wachsende Bereitschaft, Gesetze zu verabschieden. Doch die Umsetzung ist eine andere Geschichte." Nur neun afrikanische Länder haben laut UNCTAD Behörden, die über den Datenschutz wachen. 2017 stellte Deloitte in einem Bericht fest, dass Länder wie Südafrika, Kap Verden, Madagaskar, Mali oder Südafrika die entsprechenden Gesetze nur „minimal" anwenden. Ghana und Mauritius schnitten besser ab. In vielen Ländern sind die zuständigen Behörden noch im Aufbau, oft fehlt es an qualifiziertem Personal, das Wissen über den Datenschutz ist gering. Barayre erläutert: „Für viele Entscheidungsträger und Regierungen ist es immer noch schwierig zu verstehen, welche Revolution die Digitalisierung bedeutet."

Die Diskussion über Datenschutz wird auch gegen Grundrechte instrumentalisiert, so Allie Funk von der US-Menschenrechtsorganisation Freedom House: „Viele Regierungen erkennen, dass es einen Hunger nach mehr Datenschutz gibt und wollen diesen Hunger für ihre Zwecke nutzen. Gerade autoritäre Regime verfolgen nur zu gern, was kritische Journalisten, Oppositionspolitiker oder Menschenrechtsaktivisten im Netz so treiben. Solche Gesetze erleichtern es Regierungen, auf Daten zuzugreifen, statt die Daten zu schützen." Datenschutzgesetze würden manchmal Überwachung erleichtern, zum Beispiel wenn die Regeln beinhalten, dass Daten nur im Land selbst gespeichert werden dürfen und für einen bestimmten Zeitraum aufbewahrt werden müssen. Gerade das kenianische Datenschutzgesetz beobachten die Experten von Freedom House mit großem Interesse. Viele Vorschriften darin seien sinnvoll, sagt Funk. Aber es komme auf die Umsetzung an. Funk: „Wir sehen in Kenia gerade auch einen besorgniserregenden Trend, den Cyberspace stärker zu überwachen." Letztlich gebe es für Betroffene nur einen wirksamen Schutz: Die User selbst müssten die Kontrolle darüber haben, was wo über sie gespeichert wird, und im Zweifelsfall verlangen dürfen, dass diese Daten gelöscht werden (Pelz, Afrika: Weiße Flecken beim Datenschutz, www.dw.com 18.12.2019).

China

Gehirnwellensensoren kontrollieren Schüler

Journalisten der US-Zeitung Wall Street Journal konnten eine Schule in der Nähe von Schanghai besuchen, in der die chinesischen Kinder mit GPS-Trackern in ihren Uniformen und Gehirnwellenmessgeräten am Kopf ausgestattet sind. In den Klassenräumen sind Kameras aufgehängt, die in Zusammenhang mit Gesichtserkennungssoftware das Verhalten der Kinder überwachen, etwa wie oft sie im Unterricht auf ihr Telefon schauen. Das Ziel dieses Projekts soll es sein, die Noten der Schülerinnen und Schüler zu verbessern.

Die Mutter eines Kindes sieht durchaus Datenschutzprobleme, erklärt aber: „Wenn es der Forschung und Entwicklung unseres Landes dient, denke ich, ist es kein Problem." Die Eltern begrüßen das Experiment generell wohl mit der Hoffnung, ihre Kinder in der Schule besser dastehen zu lassen. Mehrere Milliarden US-Dollar soll die Regierung bereits in die Methode investiert haben. Beteiligt sind auch große und kleinere chinesische Unternehmen.

Die Gehirnwellensensoren werden in China hergestellt und sind mit jeweils drei Elektroden ausgestattet. Kinder tragen die Geräte wie Stirnbänder den ganzen Tag lang. Die Daten sendet das System an den Hostcomputer der Lehrkraft. Diese kann damit etwa herausfinden, welche Schüler sich konzentrieren und welche nicht bei der Sache sind. In einer Zusammenfassung wird die Leistung der gesamten Klasse zusammengefasst, inklusive der Konzentrationslevel einzelner Kinder. Einzelne Berichte können dann miteinander verglichen werden. Eltern sehen die Zusammenfassung auf ihren Smartphones und haben immer und überall eine Übersicht, welche Leistungen ihre Kinder in der Klasse erbringen.

Die verwendete EEG-Technik ist allerdings laut dem Neurowissenschaftler Theodore Zanto anfällig gegenüber kleinen Einflüssen. Sind Träger etwa in Situationen aufgebracht oder unruhig, können Ergebnisse stark verfälscht werden. Die Konsequenzen sind durch die Vernetzung für die Kinder allerdings groß: Ein Schüler sagt dazu: „Stellt euch vor, bei einer Prüfung bekommen alle eine Punktzahl von 95, aber du selbst bekommst eine 85. Würdest du dich nicht als Schlusslicht sehen?". Eine Lehrerin verteidigt das Konzept. Der psychologische Effekt der Kopfbänder allein sei ein Anreiz für die Schüler, sich mehr anzustrengen. Erste Verbesserungen bei Noten seien bereits erkennbar (Nickel, Chinesische Lehrer überwachen Gehirnwellen ihrer Schüler, www.golem.de 08.10.2019).

China

Standardisierung bei der Gesichtserkennung

In der Volksrepublik China wurde begonnen, einen nationalen Standard für Gesichtserkennungstechnologien zu erarbeiten, da deren allgegenwärtige Anwendung heftige Diskussionen über die Datensicherheit ausgelöst hatte. Zhang Wang, Vizepräsident der SenseTime-Gruppe, der führenden Einheit des staatlichen Teams, das solche Standards erstellt, erklärt: „Es wird eine Anleitung und Grundlage für die Maßstäbe der Gesichtserkennung in allen Bereichen sein, einschließlich industrieller, regionaler und organisatorischer Vorschriften." Das Team wurde im November 2019 vom National Information Security Standardization Technical Committee gebildet. Daran beteiligt sind auch der Technologiekonzern Tencent, Ant Financial (die Finanzabteilung der Alibaba Group), die Pingan Group und andere führende Unternehmen auf dem Gebiet der künstlichen Intelligenz (KI).

SenseTime wurde 2014 von Tang Xiao'ou, einem bekannten KI-Wissenschaftler und Professor an der Chinese University of Hong Kong, gegründet. Es hat sich zu einem weltweit führenden Anbieter von KI-Algorithmen für mehr als 700 Kunden entwickelt. Zu den Kunden zählen Alibaba oder der Smartphone-Hersteller Xiaomi. Zhang: „Unsere Hauptaufgabe besteht nun darin, einen Rahmen für den nationalen Standard und einen Zweijahresplan für das Team festzulegen." Derzeit sammeln und untersuchen sie Themen, die angegangen werden müssen.

Der Schritt ist auf die weit verbreitete Nutzung der Technologie im Leben der Menschen zurückzuführen, angefangen beim Entsperren von Smartphones bis hin zu Sicherheitskontrollen für die täglichen Zahlungen. Dies löse Bedenken hinsichtlich der Sicherheit personenbezogener Daten aus. Bei einer Face-Swap-App namens Zao, mit der Benutzer Prominente mithilfe künstlicher Intelligenz imitieren können, müssen z.B. die Benutzenden das Bild direkt auf der Plattform vollständig autorisieren. Als Reaktion auf diese Bedenken versprach Zhang, standardisierte Kriterien für die Erkennungsgenauigkeit, die Fähigkeit zur Erkennung von Angriffen und andere Probleme zu entwickeln, die häufig von Benutzern angesprochen werden.

Er betonte, dass sich die erste Reihe von Benchmarks auf technische Anforderungen, Erkennungsmethoden und die Verwaltung personenbezogener Daten konzentrieren werde. Er ist der Ansicht, dass die Herausforderung darin bestehen werde, die Umsetzung dieser Standards zu gewährleisten. Eine Lösung liege darin, systematische Testmethoden zur Überprüfung jeder Anforderung festzulegen, um unpraktische Anforderungen zu beseitigen. In der Zwischenzeit müsse auch die gesunde und nachhaltige Entwicklung der Technologie effektiv gefördert werden, anstatt sie durch Einschränkungen zu vereiteln.

Zhang Dapeng, Professor an der Chinese University of Hong Kong in Shenzhen, ergänzte, es sei ein Muss geworden, biologische Identifikationstechnologien in der Praxis zu schützen, da sich sonst weitere Probleme ergeben würden. Er meinte, dass Datenschutz und Sicherheit in China an Bedeutung gewinnen würden und dass der Missbrauch von solch wichtigen persönlichen Informationen wie das eigene Gesichtsbild für die Menschen immer schwieriger zu akzeptieren sei: „Es ist kein technologisches Problem mehr, sondern ein wichtiges soziales Problem, an dem sich die Regierung beteiligen muss.“ Er betonte, dass die Gesetzgebung entscheidend für die Lösung des Problems sei. Nicht erwähnt wird, dass Standards bei der Gesichtserkennung auch die staatliche Überwachung der Menschen erleichtern (China will Standards für Nutzung der Gesichtserkennungstechnologie erarbeiten, german.china.org.cn 12.12.2019).

Technik-Nachrichten

GE Healthcare-Geräte sind leicht angreifbar

Wie Heise meldet, sind verschiedene medizinische Geräte von GE Healthcare zur Überwachung von Patientinnen und Patienten unsicher und können auch von außen leicht attackiert werden. Sicherheitsforscher von CyberMDX haben insgesamt sechs Sicherheitslücken entdeckt, wobei die Attacken in vielen Fällen vergleichsweise trivial auszuführen sind. Von den Schwachstellen sind fünf mit der höchstmöglichen Risikoeinstufung (CVSS v3.0 Score 10/10) versehen. In vielen Fällen könnten Angreifer eigenen Code ausführen und die volle Kontrolle über Geräte erlangen. Attacken können aus der Ferne und ohne Authentifizierung durchgeführt werden.

Konkret betroffen sind folgende Geräte:

- ApexPro Telemetry Server, Version 4.2 und früher
- CARESCAPE Telemetry Server, Version 4.2 und früher
- Clinical Information Center (CIC), Versionen 4.X und 5.X
- CARESCAPE Telemetry Server, Version 4.3 (CVE-2020- 6962,CVE-2020-6961)
- CARESCAPE Central Station (CSCS), Version 1.X
- CARESCAPE Central Station (CSCS), Version 2.X (CVE-2020- 6962, CVE-2020-6964)
- B450, Version 2.X (CVE-2020- 6962, CVE-2020-6965)
- B650, Version 1.X (CVE-2020- 6962, CVE-2020-6965)
- B650, Version 2.X (CVE-2020- 6962, CVE-2020-6965)
- B850, Version 1.X (CVE-2020- 6962, CVE-2020-6965)
- B850, Version 2.X (CVE-2020- 6962, CVE-2020-6965)

Um bei der Attacke erfolgreich zu sein, könnten Angreifer beispielsweise einen privaten SSH-Schlüssel für den Fernzugriff aus Konfigurationsdateien extrahieren. Alternativ könnte ein Zugriff auch über hartcodierte Standard-Log-in-Daten geschehen. Darüber hinaus entdeckten die Sicherheitsforscher noch, dass eine 14 Jahre alte Version der Fernverwaltungssoftware Webmin zum Einsatz kommt, was mit einer Vielzahl aktueller Sicherheitslücken einhergeht.

Bis die vom Hersteller angekündigten Updates erscheinen, müssen Admins Geräte über Workarounds absichern. Dafür bietet die Cybersecurity and Infrastructure Security Agency (CISA) Hilfen an. So sollten Admins zum Beispiel die Standard-Passwörter zügig ändern und Geräte via Firewalls effektiv abschotten (Schirrmacher, MDhex: Angreifer könnten medizinische Geräte von GE Healthcare kontrollieren, www.heise.de 24.01.2020, Kurzlink: https://heise.de/-4645197).

Mit Federated Learning datenschutzkonforme KI

Forschende des King's College London und von Nvidia haben eine Möglichkeit entwickelt, um künstliche neuronale Netzwerke (KNN) datenschutzfreundlich stellenübergreifend zu trainieren. Dabei könnten Trainingsdaten, auch sensitive medizinische Informationen, über mehrere Klinikstandorte verteilt einbezogen werden. Die neue Technik soll es also Kliniken und medizinischen Einrichtungen erlauben, an einem KI-Modell zu arbeiten und es zu trainieren, ohne dabei die Ursprungsdaten austauschen zu müssen. Bei dieser Methodik des „föderierten Lernens“ wird ein zentraler Server erstellt, welcher einen Trainingsalgorithmus für die Künstliche Intelligenz an jedes am Projekt beteiligte medizinische Zentrum sendet. Die Kliniken wiederum trainieren das Modell auf ihren hauseigenen Datensätzen, bevor sie es an den zentralen Server zurücksenden, um es dort aggregieren zu lassen. So bleibt die Integrität der Datensätze eines jeden Klinikstandortes gewahrt.

Für die Forschenden ist das Modell der medizinische „Durchbruch“ in der KI-gestützten Gesundheitsversorgung, womit die riesigen Datenbestände me-

dizinischer Einrichtungen aufgearbeitet werden können. Bei der Präsentation ihrer Ergebnisse legten sie dar: „Föderiertes Lernen ermöglicht ein kollaboratives und dezentrales Training neuronaler Netzwerke, ohne die Patientendaten weiterzugeben. Jeder Knoten trainiert sein eigenes lokales Modell und übergibt es periodisch an einen Parameterserver. Der Server sammelt und aggregiert die einzelnen Beiträge zu einem globalen Modell, das dann mit allen Knoten geteilt wird." Der vom King's College für ihre Arbeit verwendete Datensatz wurde dem BraTS 2018 Datensatz entnommen, der MRT-Scans von 285 Patienten mit Hirntumoren enthält.

In Deutschland arbeitet das Berliner KI-Startup XAIN seit 2018 mit einer vergleichbaren Methodik, um Künstliche Intelligenz zu trainieren. Das Team um CEO Leif-Nissen Lundbaek hat sich dem datenschutzkonformen „Federated Learning" verschrieben. Die europäische Datenschutz-Grundverordnung (DSGVO) macht es vielen Unternehmen schwer, kundenbezogene Daten zu nutzen und KI-Modelle zu trainieren. XAIN löst mit seinem Federated Learning-Ansatz genau das Problem und wahrt dabei die Vertraulichkeit der zugrunde liegenden Daten. Die Infrastruktur bietet Nutzern die Möglichkeit automatisierter Compliance gemäß der DSGVO und verspricht zugleich bessere Trainingsergebnisse. Dies wird als großer Durchbruch in einem Bereich angesehen, der sonst von hohen Kosten und durch aufwendige Prozesse zur Wahrung des Datenschutzes geprägt ist. Anstatt Daten in einem zentralen KI-Modell zu anonymisieren, zu aggregieren und zu speichern, trainiert die Federated Learning-Technologie von XAIN auf der Grundlage getrennt gehaltener Datenquellen eine Vielzahl von KI-Modellen separat (Nvidia und Forscher des King's College London erzielen Durchbruch beim Training von KI-Modellen, www.finanztreff.de 15.10.2019).

Clearview betreibt weltweite Gesichtsdatenbank mit Abgleichangebot

Die Journalistin Kashmir Hill beschreibt in einer Recherche für die New York Times, dass das Unternehmen Clearview eine gigantische Datenbank mit mehr als drei Milliarden Fotos von menschlichen Gesichtern aufgebaut hat: „Das geheime Unternehmen, das die Privatsphäre, wie wir sie kennen, beenden könnte", so die Überschrift. Angeblich lassen sich mit Hilfe von Clearview Millionen Menschen innerhalb weniger Sekunden erkennen. Um seine Datenbank zu speisen, hat Clearview einen gewaltigen Datenstaubsauger entwickelt, der öffentlich zugängliche Seiten im Netz durchsucht, darunter Netzwerke wie Facebook, Youtube, Twitter und Instagram. Eine Software lädt automatisch massenhaft Fotos herunter und analysiert sie. Wenn das System Übereinstimmungen findet, liefert es weitere Fotos und persönliche Daten. Damit wird das Realität, was Marc Elsberg in seinem dystopischen Roman „Zero" 2014 beschreibt.

Gemäß dem Pressebericht nutzen mehr als 600 Behörden das Angebot gegen Bezahlung, darunter das FBI, das US-amerikanische Ministerium für Innere Sicherheit, dutzende Polizeidienststellen und kanadische Ermittler, die damit Sexualverbrechen und Kindesmissbrauch aufzuklären versuchen. Die Herausgabe einer vollständigen Liste seiner Kunden verweigert Clearview bislang. Dem Bericht zufolge arbeitet die Firma aber auch mit privaten Unternehmen zusammen. Clearview war bislang praktisch unbekannt und gibt sich Mühe, dies zu bleiben: Auf der Webseite und in Geschäftsunterlagen fanden sich falsche Adressen – angeblich ein Tippfehler. Das einzige Linkedin-Profil, das einen Verweis auf Clearview enthält, gehört einem gewissen „John Good". Tatsächlich steckt dahinter Firmengründer Hoan Ton-That, der einen falschen Namen nutzte. Als Journalistin Hill dem Unternehmen nachspürte, erhielt sie monatelang keine Antwort. Schließlich meldete sich eine Expertin für Krisenkommunikation, die ein Treffen mit Ton-That arrangierte.

Derart publikumsscheu gehen meist obskure Start-ups vor, die vollmundige Versprechungen machen, Millionen von Investoren einsammeln und dann nicht liefern. Im Fall von Clearview scheint das Gegenteil der Fall zu sein. Mehrere Ermittler werden zitiert, sie wüssten selbst nicht genau, wie Clearview arbeite. Die Resultate seien aber überzeugend. Innerhalb kurzer Zeit hätten sie Verdächtige identifiziert und Verbrechen aufgeklärt, darunter Diebstahl, Mord und Kindesmissbrauch.

Das Vorgehen von Clearview ist aus Datenschutzsicht nicht akzeptabel. Die massenhafte Datensammlung verstößt nicht nur gegen die Nutzungsbedingungen von Plattformen wie Facebook. Ton-That wird dazu wie folgt zitiert: „Viele Menschen machen das. Facebook weiß es." Es ist völlig unklar, wie sicher die Datenbank ist. Behörden speichern sensible Informationen auf den Servern eines kleinen Unternehmens, über das sie kaum etwas wissen und das keiner externen Kontrolle unterliegt. In dem System steckt ein gewaltiges Missbrauchspotenzial. Polizisten, die Zugriff auf die Software besitzen, können damit Frauen stalken, die sie auf der Straße treffen. Autoritäre Regime können Teilnehmer an Demos identifizieren, so wie es Russland bereits mit vergleichbarer Technologie vormacht.

Twitter hat das US-Unternehmen Clearview aufgefordert, die Sammlung von Fotos und anderen Medien in dem sozialen Netzwerk einzustellen und alle bislang zusammengetragenen Daten zu löschen. Mit dem Zusammentragen der öffentlich zugänglichen Bilder werde gegen die Nutzungsbedingungen des Netzwerks verstoßen. Ob das Startup aber auf diesem Weg dazu gezwungen werden kann, die Datenbank tatsächlich zu löschen? Zwar gab es immer wieder in den USA Klagen gegen derartiges Scraping, aber LinkedIn verlor in solch einem Fall wenige Monaten zuvor vor einem Gericht in Kalifornien. Trotz Anfrage machten weder Facebook, noch Youtube oder Venmo Angaben, ob sie ähnlich gegen Clearview vorgehen wollen.

Offenbar überwacht Clearview, nach welchen Personen die Behörden suchen, wie Hill an der eigenen Person feststellen konnte: Als die Reporterin Polizisten bat, ein Foto von ihr analysieren zu lassen, habe das System keinen Treffer angezeigt, obwohl es viele Bilder von Hill im Netz gibt. Kurz darauf hatte Clearview die Ermitt-

ler angerufen und sich erkundigt, ob sie mit der Presse sprächen. Ton-That spielte den Vorfall herunter. Die Software habe nur wegen ungewöhnlicher Suchanfragen Alarm geschlagen. Ton-That bestätigte indes, dass ClearView einen Prototypen für eine Computerbrille entwickelt habe. Mit Hilfe von Augmented-Reality-Technologie könnte der Träger damit beliebige Menschen auf der Straße identifizieren, falls ihre Gesichter in der Datenbank enthalten sind. Dem Clearview-Gründer zufolge habe sein Unternehmen keine Pläne, die Brille tatsächlich auf den Markt zu bringen (Brühl/Hurtz, Ich kann dich sehen, SZ 21.01.2020, 18; Holland, Gesichtsdaten: Twitter fordert Clearview zur Löschung auf, www.heise.de 23.01.2020, Kurzlink: https://www.heise.de/-4644811).

Konsumenten-Tracking in der analogen Welt

Während im Internet Kundendaten umfassend und akribisch gespeichert und ausgewertet werden, überwiegt im stationären Handel noch weitgehend Anonymität. Doch analysieren Geschäfte die Laufwege von Verbrauchern, was sich z.B. beim Mietpreis niederschlagen kann. Dass die Menschen vielerorts gezählt werden, ist den wenigsten bewusst. Für Malls oder große Kaufhäuser ist es wichtig zu wissen, wie viele der Besucher tatsächlich auch Geld ausgeben. Mittels neuer Technologien ist es möglich zu erfassen, welche Abteilungen ein Kunde im Kaufhaus wie lange besucht.

Der Sprecher des Handelsverbands Deutschland, Stefan Hertel, erläuterte, dass für den stationären Handel Informationen über die Kundenfrequenz gerade durch die Online-Konkurrenz immer wichtiger wird: „Ohne entsprechende Besucherzahlen im Geschäft ist es sehr schwierig, ausreichend Umsatz zu generieren." So zögen in der Vorweihnachtszeit viele Menschen ohne konkrete Geschenkidee los und ließen sich in der Innenstadt inspirieren: „Profitieren können davon logischerweise nur die Läden, die auch viele Besucher anziehen."

Marco Atzberger, Mitglied der Geschäftsführung im Kölner Handelsforschungsinstitut EHI, beschreibt die Bedeutung der Frequenzmessungen für den Mietmarkt. Während Mieten häufig am Umsatz bemessen werden, werde in der Branche diskutiert, ob nicht die Anzahl der Besucher die „fairere Währung" sei. Immer häufiger bieten Geschäfte einen Lieferservice von gekauften Produkten an, während der direkte Umsatz im Laden ausbleibt.

Die Zahl der Besuchenden kann auf unterschiedlichen Wegen erfasst werden. Der Professor für Handelsmanagement an der Leipziger Handelshochschule (HHL) Erik Maier geht davon aus, dass alle größeren Einkaufszentren in Deutschland die Besucherströme messen. Neben dem Zählen von Kassenbons oder dem Abschätzen, wie viele Menschen im Laden sind, werde seit etwa 20 Jahren auch mittels Infrarot-Schranke gezählt, wie viele Menschen ein Geschäft betreten. Gerade größere Unternehmen greifen dabei auf neue Technologien zurück. So erfasst ein WLAN-Router etwa, wie viele Smartphones mit angeschaltetem WLAN versuchen, sich zu verbinden. Der Router erfasst die sogenannte Media-Access-Control-Adresse, eine Nummer, keinen Namen oder andere persönliche Daten. Dennoch können mit ausreichend Routern Bewegungsprofile der Kunden erstellt werden. Bei der Zählung über die WLAN-Plattform bestehen jedoch Unschärfen, da nicht jeder Mensch ein Smartphone mit aktivem WLAN in der Tasche hat. Relative Veränderungen, etwa wie viel mehr oder weniger Besucher eine Veranstaltung im Vergleich zum Vorjahr besuchten, können aber relativ valide dargestellt werden.

Die kamerabasierte Kundenerkennung geht noch einen Schritt weiter als die WLAN-Methode: Videokameras zählen potenzielle Kunden und erkennen Geschlecht oder ungefähres Alter, so Erik Meier: „Das ist aber in deutschen Kaufhäusern verhältnismäßig unüblich." Denn der Händler bewege sich damit immer mehr im Grenzbereich dessen, was mit Datenschutz-Vorgaben vereinbar sei. Fraglich sei etwa, ob solche Aufnahmen gespeichert werden dürfen oder ob Gesichter verpixelt und damit unkenntlich gemacht werden müssen. Atzberger von EHI beobachtet einen deutlichen Anstieg der Zählung mit Kameras. Die Technik sei sowieso zum Diebstahlschutz verbaut, mittlerweile würden Gesichter direkt verpixelt. Neben den Laufwegen könne sogar die Stimmung der potenziellen Kunden analysiert werden. Dies sei ein Vorteil in Zeiten, in denen der stationäre Handel kaum etwas zum Kaufverhalten seiner Kunden weiß. Die Speicherung der Daten sei allerdings ein heißes Pflaster: „Das möchte niemand anfassen." Zu groß sei die Angst bei den Händlern vor Kritik der Kunden, die großen Wert auf Datenschutz legen.

Die Verbraucherzentrale (VZ) Sachsen gibt sich nicht mit der bisherigen Selbstregulierung zufrieden und fordert eine entsprechende transparente und datenschutzfreundliche Regelung innerhalb der geplanten E-Privacy-Verordnung der Europäischen Union. Stefanie Siegert, Referentin für Digitales und Energie der VZ Sachsen, fordert, es müsse sichergestellt werden, dass auch durch das Tracking mit WLAN-Routern keine personenbezogenen Daten ohne Einwilligung der Kunden gespeichert werden: „Letztlich muss der Verbraucher entscheiden können, ob er überwacht werden möchte oder nicht." Es könne nicht Aufgabe des Verbrauchers sein, die WLAN-Funktion auszuschalten, um nicht vom Netzwerk eines Kaufhauses erfasst zu werden.

Erik Maier weist darauf hin, dass Verbraucher beim Online-Shopping wesentlich transparenter seien als in herkömmlichen Geschäften. Im stationären Handel erfasse unter Umständen ein Anbieter die Daten. Im Internet würden Daten, die durch Cookies bei ganz unterschiedlichen Plattformen gespeichert werden, hingegen zentral ausgewertet. Um die Datenerfassung zu umgehen, könne der Verbraucher die automatische Suche von Netzwerken in den Smartphone-Eigenschaften deaktivieren. Außerdem sei es sinnvoll, regelmäßig die Cookies im Webbrowser zu löschen (Kahnert, So werden Kunden im Geschäft heimlich gezählt, www.fr-online.de 09.12.2019).

Rechtsprechung

BVerfG

Recht auf Vergessen I und II

Das Bundesverfassungsgericht hat mit Beschluss vom 06.11.2019 entschieden, dass ein Mensch auch nach schweren Straftaten das Recht hat, online nicht dauerhaft mit vollem Namen gefunden zu werden (1 BvR 16/13). Die obersten deutschen Richter gaben der Verfassungsbeschwerde eines im Jahr 1982 wegen Mordes verurteilten Mannes statt, der sich gegen die vollständige Nennung seines Namens in online noch immer verfügbaren Presseartikeln wendet. Bei der Abwägung zwischen Persönlichkeitsrechten und Pressefreiheit muss demnach besonders der zeitliche Abstand zu einer Tat beachtet werden.

Onlinepressearchive können demnach verpflichtet sein, Schutzvorkehrungen gegen die zeitlich unbegrenzte Verbreitung personenbezogener Berichte durch Internetsuchmaschinen zu treffen. Es sei ein Ausgleich anzustreben: Der ungehinderte Zugriff auf einen Originaltext soll möglichst weitgehend erhalten bleiben. Aber im Einzelfall soll bei bestehendem Schutzbedarf der Zugriff hinreichend begrenzt werden.

Der Kläger wurde im Jahr 1982 wegen Mordes zu einer lebenslangen Freiheitsstrafe verurteilt, weil er an Bord einer Jacht zwei Menschen erschossen hatte. Wer 37 Jahre später seinen Namen in einer Internetsuchmaschine eingab, stieß nach wie vor auf kostenlos abrufbare Artikel im Archiv des „Spiegel" unter vollständiger Namensnennung. Dagegen erhob der Mann eine Unterlassungsklage. Der Bundesgerichtshof (BGH) wies diese Klage in letzter Instanz ab. Der Schutz der Persönlichkeit habe in diesem Fall hinter dem Informationsinteresse der Öffentlichkeit und dem Recht auf freie Meinungsäußerung zurückzutreten. Dagegen zog der Mann vor das Bundesverfassungsgericht, das seiner Verfassungsbeschwerde gegen das BGH-Urteil statt gab.

Das BVerfG stellte klar, dass Betroffene nicht allein über das „Recht auf Vergessenwerden" bestimmen könnten: „Welche Informationen als interessant, bewundernswert, anstößig oder verwerflich erinnert werden, unterliegt insoweit nicht der einseitigen Verfügung des Betroffenen". Aus dem allgemeinen Persönlichkeitsrecht folge nicht das Recht, alle früheren personenbezogenen Informationen aus dem Internet löschen zu lassen. Während bei aktueller Berichterstattung dem Informationsinteresse „in der Regel" Vorrang eingeräumt werde, nehme „das berechtigte Interesse an einer identifizierenden Berichterstattung mit zunehmendem zeitlichen Abstand zur Tat ab".

Die Richter ergänzen, dass Information früher nur in einem engen zeitlichen Rahmen zugänglich gewesen sei, heute aber – einmal digitalisiert und veröffentlicht – langfristig verfügbar sei. Hinzu kommt demnach der Umstand, dass insbesondere mittels Suchmaschinen solche alten Informationen direkt zugänglich bleiben. Anzustreben sei deshalb, „einen ungehinderten Zugriff auf den Originaltext möglichst weitgehend" zu erhalten, ihn aber einzelfallbezogen auch hinreichend zu begrenzen, „insbesondere gegen namensbezogene Suchabfragen". Von den Richtern hätte also in Betracht gezogen werden müssen, ob dem Spiegel Maßnahmen hätten auferlegt werden können, die Berichte schwerer auffindbar zu machen.

In einem ebenfalls am 06.11.2019 ergangenen Beschluss zum „Recht auf Vergessen" wies das BVerfG dagegen eine Verfassungsbeschwerde gegen das Oberlandesgericht (OLG) Celle ab (1 BvR 276/17). In dem Fall ging es um einen Fernsehbeitrag des NDR-Magazins Panorama, zu dem das Interview der später klagenden Beschwerdeführerin gehörte. Eine Internetsuche nach ihrem Namen führt demnach direkt zu dem Beitrag, dem sie etwa die Formulierung „fiese Tricks" im Titel vorwirft. Ihr Versuch, das gerichtlich zu verhindern, war gescheitert und die Karlsruher Richter konnten keinen Fehler des OLG erkennen. Ein Anspruch auf Auslistung sei im konkreten Fall „jedenfalls zum gegenwärtigen Zeitpunkt noch nicht gegeben" (Bundesverfassungsgericht stärkt Recht auf Vergessen im Internet, www.zeit.de 27.11.2019; Holland, „Recht auf Vergessen" auch bei schweren Straftaten, www.heise.de 27.11.2019, Kurzlink: https://heise.de/-4597240)

BVerwG

Auswahlermessen für Datenschutzaufsicht

Am 11.09.2019 hat das Bundesverwaltungsgericht (BVerwG) in Leipzig entschieden, dass eine Datenschutzbehörde den Betrieb einer Facebook-Fanpage untersagen kann (6 C 15.18). Damit erging die nächste Entscheidung in dem inzwischen über 8 Jahre dauernden Verfahren zwischen der Wirtschaftsakademie Schleswig-Holstein und dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD). Nachdem der EuGH entschieden hatte, dass ein Betreiber einer Facebook-Fanpage für die Datenerhebung verantwortlich ist (dazu Weichert, DANA 1/2019, 4 ff.), musste jetzt das vorlegende BVerwG seine Entscheidung treffen, bei der es nicht um die Frage der Rechtmäßigkeit des Fanpage-Betriebs ging, sondern ausschließlich um prozessuale Vorfragen, nämlich darum, ob das ULD als Datenschutzbehörde überhaupt befugt war, die Deaktivierung der Fanpage von der Wirtschaftsakademie zu verlangen. Das wurde vom BVerwG bejaht. Es ließ sich dabei vom Gedanken der Effektivität zur Abwehr von Gefahren im Datenschutzbereich leiten:

„[...] Für die Auswahl unter mehreren datenschutzrechtlich Verantwortlichen erweist sich der das Gefahrenabwehrrecht beherrschende Gedanke der Effektivität als legitim. Die Behörde kann sich bei der Auswahl unter mehreren in Betracht kommenden Adressaten von

der Erwägung leiten lassen, dass ein rechtswidriger Zustand durch die Inanspruchnahme eines bestimmten Adressaten schneller oder wirksamer beseitigt werden kann. […]" (Rn. 30).

„Auch im Bereich des Datenschutzes kann es das Gebot einer effektiven und wirkungsvollen Gefahrenabwehr rechtfertigen, denjenigen Verantwortlichen heranzuziehen, dessen Pflichtigkeit sich ohne weiteres bejahen lässt und dem effektive Mittel zum Abstellen des Verstoßes zur Verfügung stehen. […]" (Rn. 31).

Über die Rechtskonformität der konkreten Anordnung aus dem Jahr 2011 hat nun das Oberverwaltungsgericht Schleswig zu entscheiden. Das BVerwG betonte allerdings die Konsequenz, sollte die Rechtskonformität der Anordnung des ULD bestätigt werden: „Hat diese Maßnahme Bestand, so wird sich Facebook um eine datenschutzrechtskonforme Lösung bemühen müssen, um sein Geschäftsmodell in Deutschland weiterverfolgen zu können."

Marit Hansen, Landesbeauftragte für Datenschutz Schleswig-Holstein, freut sich über das Urteil, mit dem „mehr Klarheit für die Anwendung unseres aufsichtsbehördlichen Instrumentariums, besonders wenn mehrere datenschutzrechtliche Verantwortliche an einer Datenverarbeitung beteiligt sind", hergestellt werde (ULD, Facebook-Fanpage-Verfahren: Urteil des Bundesverwaltungsgerichts spricht deutliche Sprache, PE 05.12.2019).

LAG Mecklenburg-Vorpommern

Schadenersatz wegen unzulässiger Videoüberwachung

Das Landesarbeitsgericht Mecklenburg-Vorpommern (LAG) sprach einem Beschäftigten wegen einer unzulässigen Videoüberwachung durch seinen Arbeitgeber einen Schadenersatzanspruch nach § 823 BGB wegen Verletzung von Persönlichkeitsrechten zu (Az., 2 Sa 214/19). Der Mitarbeiter einer Tankstelle beendete sein Arbeitsverhältnis, nachdem er sich durch massive Videoüberwachung in seinen Persönlichkeitsrechten verletzt sah. Ihn störten weniger die sichtbaren Kameras im öffentlichen Bereich (Zapfsäulen, Verkaufsraum), die vor allem auf die Abwehr von Straftaten Außenstehender zielen, sondern vor allem versteckte Kameras im Kassen- und im Lagerbereich, die nach seiner Einschätzung ausschließlich auf ihn und die Kollegen als Arbeitnehmer der Tankstelle abzielen.

Das LAG gab dem Angestellten Recht. Durch die Installation der versteckten Kameras im Flur- und Lagerbereich habe der Arbeitgeber die Persönlichkeitsrechte des Angestellten verletzt. Wegen der nur kurzen Dauer des Beschäftigungsverhältnisses hielt das Gericht einen Schadenersatz in Höhe von 1.500 Euro für gerechtfertigt. Es gehört zum Persönlichkeitsrecht jedes Beschäftigten, dass dieser grds. selbst bestimmen kann, ob er abgefilmt wird oder nicht. Nur im Ausnahmefall sind Film- oder Videoaufnahmen durch den Arbeitgeber zulässig.

Da der Einsatz der versteckten Deckenkameras im Flurbereich nicht auf externe Straftäter abzielte, nahm das Gericht an, dass Vermögensgegenstände, die im Sichtbereich der Kameras lagern (insbesondere Geld, Zigaretten und Alkohol), vor rechtswidrigen Zugriffen durch die Beschäftigten geschützt werden sollten. Für diese Mitarbeiterüberwachung bedürfe es nach dem BDSG einer Rechtsgrundlage. Diese könne vorliegen, wenn es einen Anlass für Verdachtsmomente gibt oder die Beschäftigten eingewilligt haben.

Eine anlasslose Überwachung der Belegschaft zum Schutz vor Vermögenschädigungen des Arbeitgebers sei verboten. Das war nach dem alten § 32 BDSG so und gilt auch heute unter dem neuen § 26 BDSG. Es habe keine konkreten Anhaltspunkte gegeben für ein berechtigtes Misstrauen gegenüber den Angestellten, dass diese beispielsweise einen Diebstahl oder sonst ein Delikt begehen könnten. Eine Einwilligung als Rechtsgrundlage sah das Gericht auch nicht. Für die Wirksamkeit einer „informierten Einwilligung" sei es erforderlich, dass der Arbeitnehmer vor Abgabe der Einwilligungserklärung über die beabsichtigte Datenverwendung informiert wird. Das Gericht konnte nicht erkennen, dass der Arbeitgeber den Beschäftigten entsprechend informiert und dieser seine Einwilligung zur Videoüberwachung abgegeben hat. Eine konkludente Einwilligung sei nicht zulässig (1.500 € Schadensersatz wegen unzulässiger Videoüberwachung, www.bund-verlag.de 12.11.2019).

OLG Naumburg

Apotheken-Internetwerbung ohne explizite Einwilligung ist wettbewerbswidrig

Das OLG Naumburg hat mit Urteil vom 14.11.2019 entschieden, dass ein Verstoß gegen DSGVO-Vorgaben wettbewerbswidrig ist und Mitbewerbern ein Unterlassungsanspruch zusteht, wenn die verletzte Norm im konkreten Fall als Marktverhaltensregelung einzuordnen ist (Az. 9 U 24/19). Im konkreten Fall betreibt der Kläger eine Apotheke. Der Beklagte ist ebenfalls Apotheker und betreibt eine Apotheke, die im Internet wirbt. Der Beklagte handelt sein Sortiment, also auch apothekenpflichtige Medikamente, außerdem auch über die Internet-Plattform „Amazon Marketplace". Der Kläger hatte den Beklagten am 16.06.2017 wegen des Vertriebs über diese Plattform abmahnen lassen und eine strafbewehrte Unterlassungserklärung gefordert.

Der Vertrieb über die genannte Plattform verstoße gegen Datenschutzrecht und die Berufsordnung der Apotheker und sei daher wettbewerbswidrig. Für die im Zusammenhang mit dem Erwerb apothekenpflichtiger Medikamente einhergehende Verarbeitung gesundheitsbezogener Daten des Kunden fehle es an einer vorherigen schriftlichen Einwilligung, da diese beim Bestellprozess nicht eingeholt werde.

Das OLG Naumburg folgte der Entscheidung der Vorinstanz, dem Landgericht Stendal. In der vorliegenden Fallkonstellation seien die Regeln der DSGVO als Marktverhaltensregeln im Sinne des § 3a UWG (Gesetz gegen den unlauteren Wettbewerb) anzusehen. Bei den erfassten Daten handelt es sich um Gesundheitsdaten im Sinne von Art. 9 Abs. 1 DSGVO. Der Beklagte verarbeitet die von der Handelsplattform erhobenen Daten ohne ausdrückliche Einwilligung im Sinne des Art. 9 Abs. 2 lit. a DSGVO.

Die Frage, ob Datenschutzbestimmungen nach Inkrafttreten der DSGVO Marktverhaltensregeln darstellen, ist juristisch umstritten. Das OLG Hamburg nahm nach Inkrafttreten der DSGVO an, dass insoweit die jeweilige Norm konkret darauf überprüft werden muss, ob gerade jene Norm eine Regelung des Marktverhaltens zum Gegenstand hat (OLG Hamburg, Urteil v. 25.10.2018, Az. 3 U 66/17). Das OLG Naumburg schließt sich der Auffassung des OLG Hamburg an. Im vorliegenden Fall habe der Beklagte die Plattform Amazon Marketplace in das Feilbieten der von ihm vertriebenen Medikamente und Medizinprodukte in der Weise einbezogen, dass er die Popularität dieser Plattform nutzt, um Kunden zu gewinnen. Er setzt damit die Plattform als Werbeträger ein. Amazon selbst wertet die Daten aus, um zu werben. Dies ziele auf den Markt ab und berühre die wettbewerblichen Interessen der Marktteilnehmer. Denn durch die Auswertung der Absatzdaten könnten Kunden zielgerichtet angesprochen werden.

Bei den Bestelldaten der Kunden handelt es sich um Gesundheitsdaten im Sinne von Art. 9 Abs. 1 DSGVO. Auch wenn die Daten, die Amazon für den Bestellvorgang erfasst, keine ärztlichen Befunde o.Ä. beinhalten, so könnten aus den Bestelldaten Rückschlüsse auf die Gesundheit des Bestellers gezogen werden. Insbesondere die Kombination aus mehreren apothekenpflichtigen Medikamenten lasse einen Rückschluss auf den Gesundheitszustand des Bestellers zu.

Vorliegend fehle es an einer wirksamen Einwilligung im Sinne des Art. 9 Abs. 2 lit. a DSGVO. Angesichts des Wortlauts des Art. 9 Abs. 2 lit. a DSGVO („ausdrücklich eingewilligt") dürfe eine konkludente Einwilligung die Voraussetzung dieser Vorschrift nicht erfüllen, zumal eine ausdrückliche Einwilligung gerade nicht vorliege. Darüber hinaus werde die Verpflichtung des Apothekers zur Einholung einer schriftlichen Einwilligung berufsrechtlich durch die Berufsordnung der Apothekenkammer Sachsen-Anhalt konkretisiert. § 15 Abs. 2 dieser Berufsordnung lautet: „Die Speicherung und Nutzung patientenbezogener Daten bedarf der vorherigen schriftlichen Einwilligung des Betroffenen, sofern sie nicht nach dem Bundesdatenschutzgesetz und anderen Ermächtigungsgrundlagen zulässig sind oder von gesetzlichen Bestimmungen gefordert werden" (Jöhnke, Wann ein DSGVO-Verstoß wettbewerbswidrig ist, www.asscompact.de 06.12.2019).

OLG Düsseldorf

Facebook muss Deutsch verstehen

Das Oberlandesgericht Düsseldorf (OLG) hat mit Beschluss vom 18.12.2019 (Az. I-7 W 66/19) entschieden, dass Facebook in einer gerichtlichen Auseinandersetzung mit einem deutschen Nutzer nicht auf einer Übersetzung deutschsprachiger Schriftstücke in das Englische bestehen kann. September 2018 hatte ein Mann aus Düsseldorf vor dem Landgericht Düsseldorf (LG) eine einstweilige Verfügung gegen Facebook erwirkt. Das Internetunternehmen mit Sitz in Irland hatte den Mann wegen des Einstellens eines bestimmten Textes gesperrt und den Text gelöscht. Dies wurde Facebook vom LG per einstweiliger Verfügung untersagt.

Der Mann ließ Facebook die einstweilige Verfügung zustellen. Daraufhin meldete sich allerdings eine in Dublin ansässige Kanzlei und erklärte, dass Facebook die Entgegennahme der übersandten Schriftstücke ablehne, da keine englische Übersetzung der Schriftstücke zur Verfügung gestellt worden sei und die Rechtsabteilung die deutsche Sprache nicht verstehe. Es werde eine englische Übersetzung benötigt.

Als der Mann nun rund 730 Euro für die ihm durch die Zustellung entstandenen Kosten bei der Rechtspflegerin des LG geltend machte, wies diese den Antrag zurück, schließlich sei die einstweilige Verfügung nicht wirksam zugestellt worden. Der Mann legte dann beim OLG Düsseldorf sofortige Beschwerde ein. Das OLG ließ die Argumentation von Facebook nicht gelten und hielt die Zustellung für wirksam. Für das Sprachverständnis komme es nämlich auf die Organisation des Unternehmens insgesamt an.

Das OLG führte aus, dass Facebook in Deutschland über eine Vielzahl von Nutzern verfüge, denen die Plattform vollständig in deutscher Sprache zur Verfügung gestellt werde. Auch die in diesem Zusammenhang verwendeten vertraglichen Dokumente seien in deutscher Sprache gehalten. Konkreten Formulierungen in den Nutzungsbedingungen ließen sich gründliche Kenntnisse der deutschen Sprache und des deutschen Rechts entnehmen. Die einstweilige Verfügung konnte somit auch auf Deutsch wirksam zugestellt werden. Die Entscheidung über die Kosten hat das OLG an die Rechtspflegerin des LG zurückverwiesen. Dort muss nun Facebook noch rechtliches Gehör bezüglich der Kostenfestsetzung gewährt und auch über die Kosten des Beschwerdeverfahrens entschieden werden (Facebook kann genug Deutsch, www.lto.de 07.01.2020).

VG Hamburg

G-20-Polizeifahndungsabgleich mit Gesichtsbildern zulässig

Das Verwaltungsgericht Hamburg (VG) hat mit Urteil vom 23.10.2019 entschieden, dass die Polizei zur Aufklärung von Straftaten während des G-20-Gipfels in Hamburg im Juli 2017 weiter auf eine Datenbank zum Massenabgleich biometrischer Gesichtsdaten zurückgreifen darf und damit die Anordnung des Hamburger Datenschutzbeauftragten aufgehoben, diese sogenannte Referenzdatenbank zu löschen (Az. 17 K 203/19). Die Richter stuften diese Anordnung als rechtswidrig ein. Grundlage für die Entscheidung des Verwaltungsgerichts war eine Klage des Hamburger Innensenators. Für die Anordnung des Datenschutzbeauftragten lagen nach Ansicht des Gerichts die Voraussetzungen nicht vor. Dieser hätte die Datenverarbeitung der Polizei in der konkreten Form in den Blick nehmen und eigene Feststellungen zu einem Verstoß gegen Vorschriften des Datenschutzes treffen müssen. Eine Berufung ließ das Gericht nicht zu. Der Datenschutzbeauftragte könnte jetzt noch einen Antrag auf Zulassung der Berufung beim Oberverwaltungsgericht Hamburg stellen.

Die Hamburger Polizei setzt zur Aufklärung der schweren Ausschreitungen

beim G20-Gipfel auch auf Gesichtserkennungssoftware (DANA 4/2018, 199). Hamburgs Datenschutzbeauftragter Johannes Caspar ging davon aus, dass das Erheben und Speichern der Bild- und Videodateien von Personen, die beim G20-Gipfel Straftaten begangen haben, durch die Polizei zulässig war. Dies aber gelte aber nicht für die biometrische Verarbeitung dieses Rohmaterials durch den Einsatz einer Gesichtserkennungssoftware: „Daten von größtenteils völlig unbeteiligten Personen werden biometrisch verarbeitet und zum Zweck der Strafverfolgung gespeichert."

Caspar zeigte sich von der Entscheidung des VG enttäuscht. Das Gericht beschränke die Kompetenz des Datenschutzbeauftragten offenbar „auf eine Überprüfung der Datenverarbeitung in konkret praktizierter Form und auf Verstöße gegen einzelne Datenschutzgesetze". In „Fällen, in denen die Datenverarbeitung durch die verantwortliche Stelle ohne gesetzliche Grundlage erfolgt und damit ein gesetzlicher Überprüfungsrahmen gerade fehlt", sei dies „problematisch und widersprüchlich". Die Entscheidung des Gerichts mache den Weg dafür frei, dass „zur Strafverfolgung künftig alle erdenklichen Daten aus dem öffentlichen Raum" gesammelt und zum Generieren biometrischer Profile genutzt werden, „ohne dass konkrete gesetzliche Vorgaben eine unabhängige Kontrolle zur Sicherung von Rechten Betroffener ermöglichen" (G20 in Hamburg Polizei darf Datenbank für Gesichtsabgleich weiter nutzen, www.spiegel.de 4.10.2019).

VG Schleswig

Videoüberwachung in Fitness-Umkleiden unzulässig

Mit Urteil vom 19.11.2019 hat das Verwaltungsgericht Schleswig (VG) die Klagen des Betreibers einer Fitness-Kette gegen die Anordnungen der Datenschutzbehörde Schleswig-Holstein zum Abbau von Videokameras in Umkleidekabinen verhandelt und abgewiesen (Az. 8 A 832-825/17). Einige Jahre zuvor hatte die Behörde, das Unabhängige Landeszentrum für Datenschutz (ULD), Fitness-Studios geprüft und für alle vier Studios festgestellt, dass die Videoüberwachung in einigen Bereichen gegen das Datenschutzrecht verstößt. Das ULD untersagte im Juni 2017 die Überwachung dieser Bereiche. Betroffen sind Videokameras in Umkleiden, auf Trainingsflächen und in Aufenthaltsbereichen. Marit Hansen, die Leiterin des ULD, berichtet, dass Sporttreibende und Fitness-Fans sich immer wieder beim ULD über Videokameras in Fitness-Studios beschweren: „Nicht jede Videokamera ist unzulässig, aber in Umkleiden, in denen sich die Sportlerinnen und Sportler umziehen, haben sie überhaupt nichts zu suchen. Unser Prüfteam hat sich damals die Kameras genau angeschaut und bewertet. Nach der jetzigen Bestätigung durch das Verwaltungsgericht erwarte ich eine zügige Umsetzung der Datenschutzanforderungen. Es gilt nämlich: Eine Beobachtung und Aufzeichnung durch Videokameras beeinträchtigt die Privatsphäre – hier müssen Betreiber immer die schutzwürdigen Interessen der Menschen berücksichtigen" (ULD PM 20.11.2019, Videoüberwachung im Fitness-Studio – nicht in Umkleiden!).

AGH Berlin

Keine Ende-zu-Ende-Verschlüsselung für Anwälte

Der Berliner Anwaltsgerichtshof (AGH) hat am 14.11.2019 die Klage einer Gruppe von Rechtsanwälten abgewiesen, die gefordert hatten, das „besondere elektronische Anwaltspostfach" (beA) nachträglich mit einer sicheren Ende-zu-Ende-Verschlüsselung auszurüsten (I AGH 6/18). Das Gericht hält es im Gegensatz zu den Antragstellern nicht für nötig, für das digitale Kommunikationsverfahren eine solche Verschlüsselung vorzuschreiben.

Der AGH begründet seinen Beschluss damit, dass es sich bei „Sicherheit" um einen unbestimmten Rechtsbegriff handele. Um diesen anzuwenden und auszulegen, müssten Sinn und Zweck des Gesetzes und die geschützten Rechtspositionen der Kläger abgewogen werden. Es gehe nur darum, einen relativen Zustand der Gefahrenfreiheit zu gewährleisten. Dem genügten die derzeitigen Vorkehrungen. Aus den rechtlichen Regelungen zum Anwaltspostfach geht nach Ansicht des Gerichts nicht hervor, dass eine solche durchgängige Verschlüsselung zwingend notwendig ist.

Rechtsanwälte müssen das äußerst umstrittene und pannenanfällige beA u.a. für elektronische Gerichtspost nutzen. Die Konzeption der Bundesrechtsanwaltskammer (BRAK) sieht aber keine durchgehende kryptografische Absicherung ausgetauschter Nachrichten und Dateien vor, die sicherstellen würde, dass nur der Versender und der vorgesehene Empfänger mitlesen können.

Die Kommunikation lässt sich in dem System unterwegs auf einem Server der BRAK mit einem Hardware-Sicherheitsmodul (HSM) „umschlüsseln", was die durchgehende Vertraulichkeitskette durchbricht. Mit der Option zum zeitweiligen Ent- und späteren Wiederverschlüsseln ist ein Zugriff auf sensible Nachrichten innerhalb des HSM zumindest technisch denkbar, was gerade angesichts des lohnenden Ziels Angreifer auch aus dem kriminellen Milieu anlocken könnte. Trotz dieser Konstruktion hatte die Bundesrechtsanwaltskammer ursprünglich fälschlicherweise behauptet, dass das BeA eine Ende-zu-Ende-Verschlüsselung nutzt.

Ulf Buermeyer, Vorsitzender der die Klage unterstützenden und koordinierenden Gesellschaft für Freiheitsrechte (GFF), wertete das erstinstanzliche Urteil als „Rückschlag für die IT-Sicherheit im Rechtsverkehr und damit auch für die Integrität des Rechtsstaats insgesamt". Der AGH weiche damit die gesetzliche Pflicht zum Schutz des elektronischen Verfahrens nach dem Stand der Technik unnötig auf. Letztlich ließen die Richter so ein „halbwegs sicheres beA" genügen, obwohl mit einer durchgehenden Verschlüsselung seit Jahrzehnten die Möglichkeit für wirklich sichere Kommunikation zur Verfügung stünde.

Die GFF prüft, ob eine Berufung sinnvoll ist. Buermeyer zeigte sich vorab bereits sehr zuversichtlich, dass zumindest „der Bundesgerichtshof das beA in seiner derzeitigen Form wie wir als gesetzwidrige Gefahr für die Vertraulichkeit der anwaltlichen Kommunikation erkennen wird" (Krempl, Gericht: Durchgehende Verschlüsselung beim Anwaltspostfach nicht nötig, www.heise.

de 14.11.2019; Böck, Keine Ende-zu-Ende-Verschlüsselung fürs Anwaltspostfach, www.golem.de 14.11.2019).

Österreichischer VerfGH

Staatstrojaner und Kfz-Kennzeichen-Speicherung verfassungswidrig

Der österreichische Verfassungsgerichtshof hat mit Urteil vom 11.12.2019 Teile des von den damaligen Regierungsfraktionen ÖVP und FPÖ beschlossenen „Sicherheitspakets" gekippt (G 72-74/2019, G 181-182/2019). Wie das Gericht am 11.12.2019 bekanntgab, wurden der von der letzten rechtskonservativen Regierung 2018 eingeführte „Bundestrojaner" sowie die automatische Kennzeichenerfassung für verfassungswidrig erklärt. „Die verdeckte Überwachung verschlüsselter Nachrichten" durch Behörden mittels des „Bundestrojaners" sei ein zu starker Eingriff in die Privatsphäre, da auch viele unbeteiligte Kontakte der Überwachten mitbetroffen wären. Auch sei nicht gewährleistet, dass solche Überwachungsmaßnahmen nur bei schweren Straftaten angewendet würden, die eine so weitgehende Überwachung rechtfertigen könnten. Dass die Sicherheitsbehörden zur Installation des Trojaners auf Geräten von Zielpersonen heimlich in Wohnungen eindringen und etwaige Sicherheitsvorkehrungen aushebeln dürften, verstoße außerdem gegen die Unverletzlichkeit des Hausrechts.

Die Regierung unter Bundeskanzler Kurz hatte die Befugnisse für Sicherheitsbehörden stark ausgeweitet, um das Mitlesen verschlüsselter Messenger-Kommunikation direkt an der Quelle zu ermöglichen. Die Einführung wäre im April 2020 für Verbrechen mit einer Höchststrafe von mehr als zehn Jahren oder bei Terrorverdacht und bei Straftaten gegen Leib und Leben sowie Sexualdelikten mit einer Höchststrafe von über fünf Jahren geplant gewesen.

Ebenso kippten die Richter den Zugriff der Behörden auf Kameras an österreichischen Straßen, um Kennzeichen, Autotyp, Marke und Farbe sowie die Identität der Fahrer erfassen und zwei Wochen lang speichern zu dürfen. Die damit entstehende anlasslose Vorratsdatenspeicherung sei unverhältnismäßig, die permanente Datenerfassung im Straßenverkehr könnte bei weiten Teilen der Bevölkerung ein „Gefühl der Überwachung" erzeugen. Dieses Überwachungsgefühl könne die Versammlungs- oder Meinungsfreiheit einschränken. Darüber hinaus sei die Ermittlungsmethode alleine schon unverhältnismäßig, da auch schon Fälle „der leichtesten Vermögenskriminalität" verfolgt werden dürften.

Teil der nun gestoppten Straßenüberwachung ist auch, dass die Behörden nicht mehr verdeckt auf die Daten des „Section Control"-Systems zugreifen dürfen, das primär Geschwindigkeiten auf einer bestimmten Wegstrecke misst. Da damit Standortdaten und ein Bewegungsprofil erstellt werden könnten, handele es sich laut den Richtern um einen „gravierenden Eingriff" in Datenschutz und Privatsphäre.

Die Opposition hatte beim Beschluss des Überwachungspakets im April 2018 gewarnt, Österreich werde dadurch zu einem „Überwachungsstaat". Die Klage vor dem Verfassungsgerichtshof hatten daraufhin Abgeordnete der SPÖ und der liberalen Neos eingereicht. Der stellvertretende Neos-Chef Niki Scherak sah in dem Urteil eine „klare Absage an die umfassenden Überwachungsfantasien" der damaligen türkis-blauen Regierung. Von dem beschlossenen Paket bleiben nur noch einige andere Regelungen übrig. So haben Strafermittler weiterhin Zugriff auf zahlreiche Videokameras im öffentlichen Raum, wie zum Beispiel in Bahnhöfen und Flughäfen. Zulässig bleiben eine Identifizierungspflicht beim Kauf von SIM-Karten sowie ein gelockertes Briefgeheimnis (Koenigsdorff, Österreichisches Verfassungsgericht stoppt Staatstrojaner, www.heise.de 11.12.2019, Kurzlink: https://heise.de/-4612129).

Buchbesprechungen



Hauser/Haag
Datenschutz im Krankenhaus – mit allen Neuerungen durch die DS-GVO, 5. Auflage 2019, 662 Seiten,
ISBN 978-3-946866-17-6, 64,90 €

(wh) Das umfangreiche Werk gibt einen umfassenden Überblick über die datenschutzrechtlichen Grundlagen, die bei der Patientendatenverarbeitung zu beachten sind. Hierbei finden neben der EU-Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz 2018 (BDSG) auch landes- und bereichsspezifische Regelungen wie Sozialgesetzbuch (SGB) V, Landeskrankenhaus- und -datenschutzgesetze, kirchliches Datenschutzrecht und die ärztliche Schweigepflicht Beachtung. Auf eine kurze Behandlung der Grundlagen des Datenschutzes folgt eine ebenfalls kurze Erörterung des zentralen Begriffs der „Verarbeitung". Daran schließt sich ein Überblick über die anzuwendenden Datenschutznormen und -regelungen an. Die Themen „Einwilligung" sowie „Ärztliche Schweigepflicht" werden im ausreichenden Umfang erörtert. Die durch die DSGVO erweiterten Rechte der betroffenen Personen finden eine ausführliche Beachtung. Die Verwendung von Patientendaten innerhalb des Krankhauses wird, wie auch die Übermittlung von Patientendaten an Stellen außerhalb des Krankenhauses, zum einen grundsätzlich

und zum anderen mit praktischen Fallbeispielen erläutert. Weitere Themen wie „Dokumentation und Archivierung" und Ausführungen zu den betrieblichen Datenschutzbeauftragten runden das Werk ab. Datenschutzbeauftragten und Datenschutzverantwortlichen in Krankenhäusern hilft dieses Werk sicher bei der Umsetzung der vielfältigen Anforderungen des Datenschutzes in ihren Einrichtungen.



Stiftung Datenschutz (Hrsg.)
Dateneigentum und Datenhandel, DatenDebatten Band 3, Schriftenreihe der Stiftung Datenschutz,
2019/ 1. Auflage, 325 Seiten,
ISBN 978-3-503-18225-1, 58,- €

(wh) In neunzehn Beiträgen von Autorinnen und Autoren aus unterschiedlichen Disziplinen werden die Themen Dateneigentum und Datenhandel sowie damit verbundene Aspekte erörtert. Einigkeit besteht darin, dass es im Sinne des Materialgüterrechts kein Eigentum an Daten geben kann. In Bezug auf das Immaterialgüterrecht gehen die Meinungen hingegen auseinander. Zum einen wird darauf verwiesen, dass es ähnlich zum Begriff „geistiges Eigentum" im Sinne des Urheberrechts ein Dateneigentum geben könnte. Auf der anderen Seite wird argumentiert, dass es bei vielen Daten, seien sie personenbezogen oder nicht, an einer Urheberschaft fehle. Gerade bei personenbezogenen Daten – die im Kontext des Herausgebers besonders interessant sind – stellt sich die auch in diesem Werk erörterte Frage, wer denn Eigentum an den Daten erwirbt: Die betroffene Person, auf die sich die Daten beziehen? Das Unternehmen, das die Daten zu seinen Zwecken erhebt? Auch die Fragestellungen, welche Bedeutung die Frage der KI in Bezug auf Dateneigentum hat, wie das Datenschutzrecht bei personenbezogenen Daten oder das Recht im Bereich von Betriebs- und Geschäftsgeheimnissen mit dem Dateneigentum verknüpft werden kann, welche Anforderungen an ein Dateneigentum es aus Verbraucherschutzsicht gibt, werden in diesem interessanten und lesenswerten Band erörtert. Durch die Bandbreite der Beiträge ist dieses Werk allen zu empfehlen, die sich mit dem Thema Dateneigentum näher beschäftigen wollen oder sich auch nur einen Überblick über die aktuelle Debatte verschaffen wollen.

Cartoon

ICH HABE DAS GEFÜHL, DASS IN SCHWEDEN TRANSPARENZ MEHR GILT ALS DATENSCHUTZ. DAS BARGELD IST WEITGEHEND ABGESCHAFFT UND SOMIT WIRD DAS KOMPLETTE KONSUMVERHALTEN PROTOKOLLIERT. AUSSERDEM KANN JEDER EINSICHT IN DIE GEHÄLTER ODER SCHULDEN DER NACHBARN BEKOMMEN UND Z. B. AUSKUNFT ERHALTEN, WELCHE FAHRZEUGE ANGEMELDET SIND.[1]

IN MANCHEN FÄLLEN WIRD DORT TRANSPARENZ – VOR ALLEM WENN ES WIE BEI WIKILEAKS UM DIE AUFDECKUNG VON KRIEGSVERBRECHEN GEHT – GAR NICHT GERN GESEHEN. DAZU WERDEN AUCH SCHON MAL POLIZEIPROTOKOLLE UMGESCHRIEBEN. EIN KLARES BEISPIEL FÜR DOPPELMORAL. SCHWEDEN TRÄGT EINE ERHEBLICHE MITSCHULD AN DER INHAFTIERUNG VON JULIAN ASSANGE IN LONDON.[2]

1 https://www.spiegel.de/karriere/gehaelter-in-schweden-maximale-transparenz-a-881340.html

2 https://www.n-tv.de/politik/Vergewaltigungsvorwuerfe-waren-konstruiert-article21611834.html

Darf der Staat auch die intimste Privatsphäre mit dem Argument „rechtsfreier Raum“ abschaffen?